http://doi.org/10.56123/percursos.2022.n12.78

A Publicidade e a Proteção de Dados Pessoais – O RGPD

Luísa Sousa[a] *

[a] ISCET – Instituto Superior de Ciências Empresariais e do Turismo, Porto, Portugal

Info

Palavras-chave:
Proteção de Dados
Publicidade
Titular de dados
Segurança

Resumo

O Regulamento Geral de Proteção de Dados é um instrumento legislativo da UE que visa a uniformização legislativa sobre o tratamento de dados pessoais dos cidadãos da União Europeia. Como princípios orientadores fundamentais inerentes ao regime estabelecido estão o reforço da segurança e da confiança do titular dos dados, bem como a limitação às finalidades específicas a que tal tratamento se dirige. Um forte quadro fiscalizador e sancionatório leva a que todos os responsáveis pelo tratamento de dados se defrontem agora com uma regulamentação mais exigente relativamente à qual terão que definir estratégias de comunicação comercial e de transmissão de dados mais rigorosas. A figura do Encarregado de Proteção de Dados é no âmbito da fiscalização e do relacionamento com as autoridades nacionais responsáveis pelo cumprimento da lei, determinante para a responsabilização e implementação de todo o processo definido e consagrado na regulamentação Europeia e Nacional.

1. Introdução

Propomo-nos neste artigo tratar o tema da Proteção de Dados não só numa perspetiva de análise legislativa sobre os principais conceitos e soluções acolhidas, mas também dar um contributo crítico sobre o regime legal decorrente das orientações impostas pelo Regulamento Geral da Proteção de Dados - Regulamento (UE) nº 679/2016 de 27 de abril, do Parlamento e do Concelho Europeu (RGPD).

Na verdade, a cada vez mais acentuada evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. Temas como a recolha e a partilha de dados pessoais registaram uma importância significativa. As novas tecnologias tornaram possível que as empresas privadas e as entidades públicas utilizem dados pessoais numa escala sem precedentes no exercício das suas atividades. Por outro lado, as pessoas singulares, fruto principalmente da sua qualidade de utilizadores da Internet, disponibilizam cada vez mais as suas informações pessoais de uma forma pública e globalizada. Estas mesmas tecnologias propiciaram a transformação da economia e da vida social e deverão continuar a contribuir para facilitar a livre circulação de dados pessoais na União Europeia e a transferência dos mesmos para países terceiros e organizações internacionais. É, pois, absolutamente necessário que se assegure um elevado nível de proteção dos dados pessoais, através da existência de conjunto de medidas de proteção de dados sólido e coerente, baseado na aplicação rigorosa das regras, por forma a gerar a confiança necessária ao desenvolvimento da economia digital. Por outro lado, não devemos esquecer que, as pessoas singulares, os operadores económicos e até as autoridades públicas, devem ter a possibilidade de controlar a utilização que é feita dos seus dados pessoais, concedendo-lhes, e até reforçando, a sua segurança jurídica.

Nesta linha, entendemos que a temática aqui tratada assume relevância a acuidade para que lhe dediquemos alguma atenção. Estruturamos o nosso texto abordando pontualmente temáticas que nos parecem importantes destacar no âmbito do referido regulamento e da Lei da proteção de dados Portuguesa.

Começamos por esclarecer alguns conceitos essenciais, como o conceito de dados pessoais, de tratamento de dados e o de consentimento. Destacamos três novos direitos, que agora integram o Regulamento: o Direito da Portabilidade dos Dados; o Direito ao Esquecimento; e o Direito de Oposição ao Tratamento de Dados.

Abordamos também os princípios e legalidade, associados ao tratamento dos dados pessoais que são recolhidos, focando assuntos tão importantes como, a finalidade do tratamento de dados, a base jurídica do tratamento e a questão do interesse legítimo. Não deixamos de dedicar algumas palavras, ainda que de forma algo superficial, à obrigação dos responsáveis de dados/subcontratantes e à proteção de dados especial, como por exemplo, os dados sensíveis.

Como se pode ler logo no considerando 1 do RGPD "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" e o considerando 4 refere que "O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser

* Endereço eletrónico: lsousa@iscet.pt (L. Sousa)

equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística."

A metodologia utilizada foi a pesquisa qualitativa, a análise legislativa e bibliográfica, a realização de investigação analítica e descritiva, respetiva interpretação e análise de conteúdos, alusivos às questões colocadas no tema que tratamos.

2. Regulamento Geral de Proteção de Dados (RGPD) Regulamento (UE) nº 679/2016 de 27 de abril: conceito, fundamentação e âmbito de aplicação

O Regulamento Geral de Proteção de Dados (RGPD) é o regulamento (UE) nº 679/2016 de 27 de abril, do Parlamento e do Conselho Europeu. Define pormenorizadamente os requisitos em matéria de recolha, armazenamento e gestão de dados pessoais, e todo o circuito dos mesmos. É aplicável tanto a empresas e organizações europeias que tratam dados pessoais na União Europeia (UE), como a empresas e organizações estabelecidas fora do território da União que tratam dados pessoais de pessoas de vivem na UE.

A necessidade de regulamentação da matéria de proteção de dados decorreu da constatação de que estava instalada uma crise de confiança no regime anterior de proteção de dados que estava a condicionar negativamente a evolução da economia digital e particularmente o desenvolvimento das empresas.

Com a evolução dos meios digitais e particularmente da internet, a recolha de dados dos consumidores passou a realizar-se cada vez mais facilmente e com um volume crescente. Quando um utilizador da internet clica em determinado campo de um website ou efetua um "post" nas redes sociais, quando recorre a uma aplicação do telemóvel ou faz algum comentário, vg. através do seu e-mail, os seus dados são recolhidos para uma qualquer outra utilização no futuro. Mais ainda, o simples facto de o sujeito colocar um "gosto" numa publicação do Facebook, do Instagram, ou do Twitter é adicionado ao seu perfil de dados e frequentemente vendido a outras empresas com o intuito de segmentar clientes, uma vez que as bases de dados vendidas possuem o perfil de público-alvo indicado para a compra dos produtos ou serviços oferecidos pela empresa compradora.

Sucede com muita frequência que os cidadãos e consumidores privados são sobrecarregados de chamadas ou emails de empresas que desconhecem completamente e com as quais nunca estabeleceram qualquer contato, com a finalidade de lhes tentarem vender determinado produto ou serviço que o mais das vezes não corresponde sequer às suas necessidades ou gostos. O consumidor vê usurpada a sua privacidade e o seu direito à reserva da vida privada com as diversas mensagens publicitárias que lhe são dirigidas sem o seu consentimento.

São estas razões, de segurança e confiança, que evidenciaram a necessidade de consumidores e empresas repensarem a questão da proteção dos dados pessoais e que levou à necessidade de rever o regime legal relativo à privacidade e segurança de dados, no sentido de o tornar mais efetivo e exequível.

De acordo com Magalhães e Pereira (2018: 17), "Após vários anos de utilização massiva da rede para comunicar, comprar, promover produtos e aproximar as pessoas e as empresas, fica o sentimento de insegurança que resulta destas relações virtuais, tendo-se considerado essencial devolver às pessoas singulares o controlo da utilização que é feita dos seus dados pessoais, devendo ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas". Na verdade, e como referimos, a grande parte dos agentes económicos e dos consumidores não estavam confortáveis e sentiam-se "abusados" na sua privacidade pela forma de tratamento dos dados pessoais que colocam na Internet. Tornou-se assim determinante implementar regras para ajudar as empresas a crescer, procurando estabelecer um conjunto de novas soluções quanto ao tratamento de dados para todas as empresas que dessem maior confiança aos negócios, ao consumidores e empresas e que permitissem maior facilidade e justiça no tráfico comercial.

Na opinião de Regente, (2015: 102) o regulamento "reforça os princípios da proteção de dados, no que diz respeito às novas tecnologias da sociedade de informação, perspetivando-se conceitos mais adequados e próximos da realidade do utilizador, e em conformidade com os direitos fundamentais da pessoa humana".

Em Portugal, até 25 de maio de 2018, esteve em vigor a Lei da Proteção de Dados Pessoais (LPDP) – Lei nº 67/98, que continha diversas regras sobre as quais os profissionais da publicidade e do marketing, entre outros, se deviam reger. A partir desta data começa a produzir efeitos o Novo Regulamento Geral de Proteção de Dados da União Europeia que consagra normas mais exigentes no que se refere à proteção do indivíduo, apostando numa fiscalização incisiva e na previsão de coimas de valores elevados que preocupam as empresas que gerem a recolha e tratamento de dados pessoais. Atualmente e na sequência da entrada em vigor do RGPD, vigora internamente a Lei 58/2019 de 8 de agosto, que nos termos do seu art. 1º "assegura a execução, na ordem jurídica interna, do 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, doravante designado abreviadamente por Regulamento Geral de Proteção de Dados (RGPD)".

De acordo com a presidente da Comissão Nacional de Proteção de Dados (CNPD), o RGPD responde à necessidade de fazer face aos riscos cada vez maiores de ameaças que ocorriam ao nível da privacidade, identidade e liberdade dos indivíduos, "renovando questões jurídicas tradicionais, mas também colocando novas questões" e novos desafios (Calvão, 2018: 21-22). De acordo com Ghosh (2018), o novo regulamento irá forçar os profissionais de marketing a diminuir drasticamente a sua dependência da recolha de dados comportamentais, pois exige o consentimento fornecido pelo cliente ou potencial cliente

de forma livre, específica, expressa, informada e inequívoca, bem como a apresentação de prova desse mesmo consentimento.
Muito haveria a dizer relativamente à concretização pela lei Portuguesa do RGPD, mas deixaremos este assunto para outra oportunidade.
O que nos propomos agora é tratar de forma sucinta e abreviada os aspetos que consideramos mais substanciais do RGPD.

3. Regulamento Geral de Proteção de Dados (RGPD) Regulamento (UE) nº 679/2016 de 27 de abril: noções relevantes

O RGPD no seu artigo 4º enumera algumas noções relevantes para o entendimento do mesmo. Selecionamos as que consideramos determinantes para este trabalho. Assim referimos a noção de "dados pessoais", com a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)". Acrescenta ainda o regulamento que "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".
São exemplos de dados pessoais, desde logo, o nome, a morada, o número do documento de identificação/ passaporte, o rendimento, o perfil cultural, o endereço IP, os dados na posse de um hospital ou médico que identifiquem de forma inequívoca uma pessoa para fins relacionados com a saúde.
Outros conceitos importantes no âmbito do RGPD a que nos devemos referir são os de:

- "Tratamento" de dados, e que o mesmo artigo considera ser "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, e exemplifica tais operações 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";
- "Responsável pelo tratamento", definido como "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais";
- "Subcontratante", "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes";
- Não podemos deixar de referir o conceito de "Consentimento" do titular dos dados, traduzido em "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;
- Finalmente o conceito de "Violação de dados pessoais", que traduz "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

4. Os princípios relativos ao Tratamento de Dados

Conforme o artigo 5º do RGPD, o tratamento de dados está sujeito a variados princípios que passamos com brevidade a enunciar. Desde logo os da licitude, lealdade e transparência, que determinam que o tratamento dos dados pelo seu responsável seja lícito, leal e transparente em relação ao titular dos dados.
Para que o tratamento dos dados pessoais se possa considerar lícito é necessário que nos termos dos art. 6º RGPD, se observe pelo menos uma das seguintes situações: exista consentimento pelo titular dos dados; se esteja perante a execução de um contrato ou do cumprimento de uma obrigação jurídica; estejam em causa a defesa de interesses vitais ou o exercício de funções de interesse público ou de exercício da autoridade pública; e finalmente que os interesses prosseguidos pelo responsável pelo tratamento ou por terceiros sejam legítimos. Além do mais é necessário que os dados se tratem com transparência e lealdade e que o seu titular possa a todo tempo ser informado e retirar o seu consentimento ao tratamento dos seus dados.
Outro dos princípios que se consagra é o da limitação da finalidade, segundo o qual os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1.
O princípio da minimização dos dados significa que estes devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados e o princípio da exatidão determina que os dados sejam exatos e atualizados sempre que necessário, particularmente a solicitação do seu titular. O responsável pelo tratamento deve adotar todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados.
Outro princípio orientador é o da limitação da conservação, segundo o qual os dados devem 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. Os dados poderão 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, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.
Finalmente, os princípios da integridade e confidencialidade**,** no sentido de estabelecer que os dados serão tratados de uma forma que garanta a sua segurança, incluindo

a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, mais uma vez adotando as medidas técnicas ou organizativas tidas como adequadas.

5. O Tratamento de Dados (Licitude do Tratamento)

Durante o tratamento, os dados pessoais podem passar por várias empresas ou organizações. No âmbito deste ciclo de tratamento de dados pessoais, há a destacar três figuras principais.

Primeiro o Responsável pelo Tratamento, que é a figura que determina a finalidade e os meios do tratamento de dados; a segunda figura é o Subcontratante, que armazena e trata dados por conta do responsável pelo tratamento; finalmente, mas de relevância significativa em todo o processo de tratamento, o Encarregado da Proteção de Dados, que pode ser designado pela empresa e é responsável por controlar o modo como os dados pessoais são tratados e por informar e aconselhar os trabalhadores que tratam dados pessoais sobre as suas obrigações. Além disso, o encarregado da proteção coopera com a autoridade de proteção de dados, no caso de Portugal, a CNPD, funcionando como ponto de contato entre esta e as pessoas singulares. Nem sempre no processo de tratamento de dados é necessária a nomeação de um encarregado de proteção de dados. Nos termos do art. 37º do RGPD, a empresa apenas tem a obrigação de designar um encarregado da proteção: se o acompanhamento de dados que fizer for regular ou sistemático; se referir a pessoas singulares ou se se tratar de categorias especiais de dados; se o tratamento dos dados for uma atividade comercial principal; se tratar dados a grande escala; e ainda se o tratamento for efetuado por uma autoridade ou organismo público.

A título de exemplo, configuremos a situação de uma empresa que trata dados pessoais para direcionar publicidade através de motores de busca (pesquisa) com base no comportamento em linha dos titulares desses dados. Sem dúvida que deve designar um encarregado da proteção de dados pois enquadra-se no art. 37º referido, já que o faz de forma sistemática e no exercício da sua atividade comercial principal. Contudo, se a empresa se limitar a enviar aos clientes material promocional uma vez por ano, já não necessitará de um encarregado da proteção de dados.

Admitamos ainda a situação um médico que recolhe dados relativos à saúde dos doentes, não precisará de um encarregado da proteção, porém se esse médico trata dados genéticos ou relativos à saúde em nome de um hospital, já será necessário um encarregado da proteção de dados já que está em causa uma categoria especial de dados e o tratamento é feito no âmbito de um hospital que é o responsável pelo tratamento de dados e que trata dados em grande escala enquadrando assim o art. 37º RGPD.

O encarregado de proteção pode ser um elemento do pessoal da organização ou pode ser contratado externamente, através de um contrato de prestação de serviços, podendo ser um indivíduo ou fazer parte ele próprio de uma organização.

6. Condições alternativas para o Tratamento de Dados

As condições que legitimam o tratamento de dados pessoais estão elencadas no art. 6º do RGPD e são entre si de verificação alternativa. Assim, para serem legítima e legalmente tratados será necessário que, no caso em concreto, se verifique uma das seguintes situações: se obtenha o consentimento do titular dos dados; que o tratamento seja necessário para executar um contrato no qual o titular dos dados é parte; que o tratamento seja necessário para cumprir uma obrigação jurídica do titular dos dados; que o tratamento seja necessário para defender os interesses vitais do titular ou de outra pessoa singular; que o tratamento seja necessário para exercer funções de interesse público ou ainda que o tratamento seja necessário no interesse legítimo da empresa, desde que os direitos e liberdades fundamentais dos titulares dos dados não sejam afetados de forma significativa.

Relativamente ao consentimento do titular de dados, o RGPD prevê regras rigorosas que visam garantir que o titular dos dados conheça de forma clara e transparente a que é que está a dar consentimento. Por isso o consentimento deve ser dado de forma livre, específica, informada e inequívoca. Deve ser solicitado pela empresa utilizando uma linguagem simples e clara. Deve ser dado através de uma atuação, v.g assinalando uma casa ou assinando um formulário, não recorrendo a formulários pré-preenchidos. A empresa só pode tratar dados se o seu titular der consentimento para o tratamento dos seus dados pessoais, e tão só para tratar esses dados de acordo com as finalidades consentidas. Finalmente importa dizer que o titular tem sempre a possibilidade de retirar o consentimento em qualquer altura.

O consentimento tem que ser informado e por isso o responsável pelo tratamento de dados deve informar de forma clara e transparente o titular dos dados sobre quem está a tratar os respetivos dados pessoais e o motivo desse tratamento. Nos termos do art. 13º do RGPD tal informação deve incluir, obrigatoriamente, os seguintes elementos: a sua identificação, a razão do tratamento dos dados, a base jurídica para o fazer e a quem se destinam os dados. Eventualmente, a informação abrangerá ainda os contactos do encarregado da proteção de dados, o interesse legítimo da empresa, sempre que invocar este fundamento jurídico para o tratamento, as medidas aplicadas para transferir os dados para um país fora da UE e se existe ou não uma obrigação legal ou contratual de fornecer os dados, no caso de decisões automatizadas, informações acerca da lógica, o alcance e as consequências da decisão. Poderá ainda abranger a indicação do período de tempo que serão conservados os dados, os direitos de proteção dos dados dos titulares (ou seja, o direito de acesso, retificação, apagamento, limitação, oposição, portabilidade, etc.), a forma como o consentimento pode ser retirado (sempre que o consentimento for o fundamento jurídico para o tratamento).

Se os dados pessoais forem relativos a crianças e se tratem com base no consentimento, (v.g. criar uma conta de rede social ou descarregar conteúdos) deve começar por obter o consentimento parental, nomeadamente através do envio de uma notificação a um progenitor/tutor. A idade até à qual um utilizador é considerado criança varia de país para país, oscilando entre os 13 e os 16 anos. Em Portugal

esta idade está fixada em 13 anos, isto é, com 13 anos completados a pessoa é autónoma para dar o seu consentimento.

7. Direitos dos Titulares de Dados

Os direitos dos titulares dos dados estão previstos nos art. 12º e ss. do RGPD.

A) Direito de Acesso aos Dados – art. 15º
Os titulares dos dados têm direito a aceder aos respetivos dados pessoais de forma gratuita. O responsável pelo tratamento dos dados pessoais, se tal lhe for solicitado pelo titular dos dados pessoais, deve dar acesso aos mesmos e nomeadamente deve dar informação sobre se os dados pessoais em questão estão a ser tratados, qual a finalidade do tratamento, categorias de dados pessoais tratados, destinatários dos dados, etc. Deve ainda fornecer-lhe uma cópia dos dados pessoais que estão a ser tratados.

B) Direito à Portabilidade dos Dados – art. 20º
Se o tratamento tiver por base o consentimento ou um contrato, o titular pode pedir que lhe sejam devolvidos os seus dados pessoais ou que sejam transmitidos a outra empresa. Os dados devem ser apresentados num formato de uso corrente que permita a leitura automática.

C) Direito a Corrigir ou Retificar os Dados – art. 16º
Se o titular dos dados considerar que os seus dados pessoais estão incorretos, incompletos ou inexatos, tem o direito de os retificar ou completar, sem demora injustificada. Se houver correção, o responsável pelo tratamento deve informar todos os destinatários com quem partilha os dados em questão de que estes foram alterados ou apagados.

D) Direito de Oposição – art. 21º
O titular dos dados pode também opor-se a qualquer momento ao tratamento dos respetivos dados pessoais para um uso específico, ainda que a empresa faça o tratamento dos dados com base no seu próprio interesse legítimo ou no exercício de funções de interesse público. Nesse caso deverá cessar o tratamento dos dados pessoais. Porém, se o interesse legítimo da empresa prevalecer sobre o interesse do titular dos dados, fica sem efeito o direito de oposição. No entanto, enquanto se determina o interesse prevalente o titular dos dados pode solicitar a limitação do tratamento dos mesmos. O direito de oposição é pleno e imediatamente eficaz no caso da comercialização direta, isto é, a empresa é obrigada a colocar termo ao tratamento dos dados pessoais sempre que o titular o solicite.

E) Direito ao Apagamento dos Dados (direito ao esquecimento) – art. 17º
O titular dos dados pode solicitar ao responsável pelo tratamento que apague os seus dados pessoais, entre outros motivos elencados no referido art. 17º, no caso de os mesmos deixarem de ser necessários para cumprir a finalidade do tratamento.
Este direito é afastado e a empresa não é obrigada a apagar os dados se o seu tratamento for necessário para respeitar a liberdade de expressão e de informação, se tiver de conservar os dados pessoais para cumprir uma obrigação legal, se existirem outras razões de interesse público para conservar os dados pessoais, tais como motivos relacionados com a saúde pública ou a investigação científica e histórica e se a conservação dos dados pessoais for necessária no âmbito de um processo judicial.
Os direitos dos titulares de dados são exercidos nos termos do art. 12º. Assim, se o titular dos dados dirigir um pedido à empresa que trata os seus dados, esta deve responder a este pedido sem demoras injustificadas no prazo de um mês a comtar da receção do pedido. Este prazo pode ser prorrogado por um período de dois meses para pedidos complexos ou múltiplos, desde que a pessoa seja informada da prorrogação.
O exercício dos direitos pelo seu titular é gratuito, não lhe podendo ser cobrada qualquer quantia por parte da empresa a quem foi efetuado o pedido. O responsável pelo tratamento de dados pode recusar o pedido do titular dos dados se este for manifestamente infundado ou excessivo, competindo-lhe a respetiva prova. Se um pedido for recusado, terá de informar o interessado das razões dessa recusa e do direito que lhe assiste de apresentar uma reclamação à autoridade de proteção de dados. Entre nós a Comissão de Proteção de Dados.

8. Manutenção de Registos pelo Responsável do Tratamento de Dados

O art. 30º do RGPD determina que a empresa que trata os dados tem o dever de estar habilitada a provar que atua em conformidade com o próprio regulamento e cumpre todas as obrigações aplicáveis, nomeadamente, na hipótese de uma inspeção da autoridade de proteção de dados.
Nesta linha, a empresa responsável pelo tratamento de dados deve conservar e manter um registo pormenorizado de elementos de vários elementos importantes. Deverá conservar os registos de dados tais como o nome e os contatos da empresa envolvida no tratamento de dados, o motivo ou motivos do tratamento de dados pessoais, a descrição das categorias de pessoas que fornecem dados pessoais, as categorias de organizações que recebem os dados pessoais, as transferências de dados pessoais para outro país ou organização, o período de conservação dos dados pessoais e a descrição das medidas de segurança utilizadas para o tratamento de dados pessoais.
A empresa deve igualmente definir e atualizar regularmente orientações e procedimentos escritos e manter os trabalhadores a par dos mesmos.
De notar que se o responsável pelo tratamento de dados for uma empresa com menos de 250 trabalhadores não necessita de conservar um registo das atividades de tratamento, desde que não proceda regularmente ao tratamento de dados e tal tratamento não ponha em risco os direitos e liberdades dos titulares dos dados em questão, bem como no caso de os dados tratados não sejam confidenciais ou registos criminais.

9. Notificação das Violações de Dados

O art. 33º do RGPD define que existe violação de dados se os dados pessoais pelos quais a empresa é responsável

forem divulgados, tanto acidental como ilicitamente, a destinatários não autorizados, forem alterados ou o acesso aos mesmos for temporariamente interrompido.
Se ocorrer uma violação de dados que represente um risco para os direitos e liberdades individuais, a empresa deve informar a autoridade de proteção de dados no prazo de 72 horas depois de tomar conhecimento da mesma. Se a violação representar um risco elevado para os titulares dos dados, a empresa será também obrigada a informar dessa violação todas as pessoas afetadas.

10. Incumprimento das Regras e Sanções

O não cumprimento do RGPD pode traduzir-se em coimas significativas, que, para determinadas infrações, podem chegar aos 20 milhões de euros ou a um valor equivalente a 4 % do volume de negócios da empresa, podendo a autoridade de proteção de dados impor sanções adicionais v.g. obrigar a empresa a pôr termo ao tratamento dos dados pessoais.
Esta imposição de sanções mais elevadas, bem como o facto de se consagrar uma vigilância mais rigorosa são respostas contidas no RGPD, que dá no entanto liberdade às autoridades de controlo dos estados membros para a concretização da aplicação de coimas que, como dissemos, poderão ascender, nos termos do art. 83º do RGPD, até aos 20 000 000 de euros ou 4% do volume de negócios anual da organização em causa referente ao ano anterior. Em todo o caso, as coimas a aplicar deverão ser "efetivas, proporcionadas e dissuasivas". Em matéria de proteção de dados e de aplicação do RGPD deixou de ser necessária a aprovação por parte das autoridades de controlo, no nosso caso da CNPD, para prosseguir com a recolha e tratamento de dados. Nos termos dos arts. 51º e 52º do RGPD, é às organizações responsáveis pelo tratamento de dados, que compete, com total autonomia, o cumprimento das normas estipuladas. O papel das autoridades é agora fiscalizador do cumprimento dessas mesmas regras com o "… fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento…". Este binómio autonomia de atuação das organizações no que respeita ao tratamento dos dados pessoais e a relevância que assume o regime de fiscalização, associado ao valor das coimas, levou a que estas se consciencializassem da necessidade, no que se refere às atividades de marketing e comunicação comercial, de reponderar as suas habituais formas de atuação.

11. As Empresas de Publicidade face ao RGPD

Independentemente do volume de negócios e da dimensão da empresa, desde que na sua atividade recolha ou processe dados pessoais, nomeadamente identificativos de clientes ou indivíduos, o RGPD é aplicável.
É então importante, deste ponto de vista, alertar particularmente as empresas publicitárias para os novos desafios no âmbito das suas ações publicitárias, de marketing, e mais especificamente de marketing digital, onde os dados pessoais e a mobilidade dos mesmos são determinantes.
É essencial uma mudança de hábitos. Era habitual que a empresa publicitária acedesse a um email ou uma listagem onde estavam incluídos dados de clientes e os utilizasse para as várias finalidades que entendia adequadas. Há agora de ter em atenção que, face ao RGPD, tem, em primeiro lugar e antes de enviar qualquer comunicação, que obter o necessário consentimento expresso do destinatário para as várias finalidades específicas. O pedir consentimento deve ser agora uma opção estratégica da empresa. Tal pedido deve ser feito de forma clara e deve ser especificada a finalidade a que se destina. O consentimento não pode ser dado por defeito, isto é, se por exemplo o consentimento for solicitado mediante uma caixa de opções, estas não podem estar pré-selecionadas, tendo que ser expressamente selecionadas pelo titular de dados.
Outro aspeto importante do pedido de consentimento é que este deve alargar-se aos meios de divulgação da comunicação, isto é, o titular dos dados deve também dar o seu consentimento quanto aos meios pelos quais se pretende divulgar a mensagem. Por exemplo, o consentimento dado para receber emails comerciais não inclui autorização para futuros contactos telefónicos, envio de SMS's ou publicidade online, etc..
Devem atender também à forma de obter o consentimento, que como vimos deverá ser inequívoco. Este caráter do consentimento não é posto em causa pela natureza concludente do comportamento que o consubstancie. Nesse sentido o artigo 217.º CC define a declaração tácita como aquela que "se deduz de factos que, com toda a probabilidade, a revelam". Assim sendo admite-se qualquer forma para prestar o consentimento, por exemplo, entre outras formas, a assinatura de um formulário, declarações orais, um comportamento concludente, o envio de um pedido de informações, na medida em que o consentimento fosse necessário para lhe dar resposta. O caráter expresso do consentimento só será exigível quando se lida com categorias especiais de dados considerados sensíveis.

12. Os Sistemas na Cloud e o Website face ao RGPD

As empresas publicitárias têm agora, com o novo sistema de tratamento de dados, de encontrar formas de aumentar a sua eficiência e rentabilidade.
Atualmente o marketing digital faz-se, em grande parte, recorrendo a processos e sistemas de automação, sendo que estes sistemas residem normalmente na *cloud* (Internet), em servidores que não são propriedade das empresas que subscrevem os serviços. Neste caso, o consentimento dado deve ser expresso para entidades terceiras.
Se por exemplo a empresa utiliza um serviço de E-mail Marketing, o titular de dados deve ter conhecimento que os seus dados são guardados fora da empresa, no caso indicado nos servidores das empresas que fornecem estes serviços. Se por exemplo a empresa opta pela criação de uma Custom Audience no Facebook, para a criação de campanhas, o que implica a importação de um ficheiro de utilizadores com os seus endereços de emails, é necessário o consentimento prévio por parte de cada um dos titulares de dados.
Se a empresa usa o seu website como um dos principais pontos de contato com os titulares dos dados, é fundamental o consentimento e a informação sobre como os dados introduzidos em formulários, são arquivados e processados, por exemplo, o envio de candidaturas, inscrições em eventos, registos de utilizadores, etc.. Caso a empresa pretenda utilizar a informação introduzida pelos

utilizadores num âmbito diferente do que está definido no local do formulário, deve solicitar o respetivo consentimento de forma clara e explícita. Assim, admitindo por exemplo que a empresa tem uma loja online e um cliente introduz os seus contatos, telemóvel, email ou morada, etc., tal não lhe confere imediatamente o direito de o adicionar à sua lista de distribuição para newsletters comerciais ou envio de SMS's, etc. Terá de obter o consentimento expresso dessa pessoa para cada finalidade.
A título de exemplo de atuação de uma empresa publicitária que seja responsável pelo tratamento de dados e para adequar a sua estratégia ao RGPD, resumimos algumas operações fundamentais no exercício da sua atividade que elencamos, ainda que, obviamente, não de forma exaustiva.
É essencial: (1) ser transparente quanto ao objetivo a atingir com a recolha dos dados pessoais; (2) disponibilizar ou apagar os dados armazenados de um indivíduo, sempre que isso lhe seja solicitado; (3) incluir no seu site um aviso sobre a utilização de ferramentas automatizadas de monitorização, explicando de que forma os dados serão tratados e para que finalidade; (4) divulgar as suas políticas de privacidade no sentido de respeitar o RGPD; (5) saber e registar onde estão armazenados os dados e quem tem o acesso aos mesmos; (6) documentar todas as informações.
Particularmente quanto às comunicações comerciais deverão sempre atuar com total transparência, nomeadamente no que se refere à publicidade comportamental que advém da publicidade online, a que já aludimos. É fundamental ter em atenção a formulação de perfis através dos dados rastreados, pois os indivíduos terão de estar claramente informados dessa formulação de perfis e têm de dar consentimento para que tal aconteça. Por último, mas não de menor importância, importa atentar no facto de que deve ser prestada a informação de forma clara acerca da instalação de testemunhos de conexão (cookies) nos seus dispositivos, que permitem monitorizar os seus comportamentos tendo de lhes ser dada a opção de aceitar ou não, ou, pelo menos, a informação da possibilidade de os remover através das definições do browser.
Terminamos com dois exemplos paradigmáticos que nos evidenciam o funcionamento do RGPD em particular nas comunicações comerciais e em particular nas comunicações publicitárias. Admitamos uma empresa de comunicações (A), que pretende sujeitar ao mesmo ato de consentimento dos seus clientes, o recebimento por estes de comunicações promocionais e publicitárias de vários bens ou serviços e a possibilidade de os mesmos serem contatados no final do período de fidelização para a renegociação dos seus contratos. Respeitará esta atuação o regime do RGPD quanto ao consentimento? Respondemos negativamente à questão porquanto estão em causa diferentes operações de tratamento de dados, com finalidades distintas, e por consequência não é possível agregá-las, de tal modo que o não consentimento em relação a uma faça decair a outra. A importância para o cliente da renegociação das condições contratuais pode limitar a liberdade de escolha em relação à outra operação de tratamento de dados.
Configuramos agora a situação de uma aplicação para telemóvel de edição de fotografias cujo acesso implica a solicitação aos utilizadores que ativem a localização por GPS para fins de prestação dos serviços. A mesma aplicação dá ainda a informação de que os dados recolhidos serão tratados para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, por isso esta solicitação vai muito além do necessário para a concretização do serviço principal prestado (edição de fotografias). Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre tal como determina o RGPD.

13. Conclusões

Como conclusão geral registamos que o Regulamento Geral da Proteção de Dados assume um papel de extrema importância no que se refere à garantia de maior segurança jurídica face à proteção de dados pessoais e nessa medida acarreta enormes vantagens sociais e económicas no âmbito do tráfico jurídico. A aplicação sua prática representou o início de um longo, global e importante percurso face à aplicação de regras impostas no âmbito de toda a União Europeia. O estabelecimento de uma aplicação uniforme das normas entre todos os Estados – Membros, regulando-se globalmente a proteção de dados representa um importante marco no respeito pelos direitos fundamentais do titular dos dados. O RGPD veio permitir aos Estados-Membros fazer face aos desafios legislativos internos, decorrentes do fenómeno digital, de uma forma mais adequada e de fácil resolução, com uma base jurídica mais sólida do que aquela que existia anteriormente. O Regulamento Geral da Proteção de Dados veio mostrar novas formas de facear as novas tecnologias. As empresas tiveram que mudar significativamente o seu posicionamento quanto à forma como recolhiam, tratavam, mantinha e utilizavam os dados dos seus fornecedores e clientes. Tiveram necessidade de se adaptar ao novo modelo europeu de proteção de dados, principalmente aquelas que utilizam a internet como um meio de informação e comunicação e, por outro lado, também já beneficiam da vantagem que daí advém.
É necessário cumprir com todas as disposições legais impostas no Regulamento pela União Europeia, assim como interpretar coerentemente o mesmo entre todos os Estados – Membros. Se isso se verificar, todos beneficiaremos com as soluções legais consagradas. Terminamos este trabalho mais conscientes do interesse e atualidade do tema tratado e de que a investigação realizada e conhecimento daí resultante superaram as nossas expectativas. Esperamos que possa servir de apoio ou suporte para quem pretende navegar no estudo desta temática tão importante do ponto de vista dos direitos humanos e fundamentais consagrados em geral no nosso ordenamento jurídico e em particular na CRP.

Referências

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS, [Consult. a 20/05/2021]. Disponível em: https://www.cnpd.pt/cidadaos/direitos/

COUTO, M. (2016), *O E-commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados - A Uniformização na*

União Europeia, Trabalho Final de Mestrado em Direito Geral, Porto, Universidade Católica Portuguesa.

GHOSH, D. (2018), "How GDPR Will Transform Digital Marketing", in *Harvard Business Review*.

JESUS, I. (2016), *O Novo Regime Jurídico de Protecção de Dados Pessoais na Europa*, Lisboa, Faculdade de Direito da Universidade Nova de Lisboa.

LOUREIRO, F. (2018), *Direito Aplicado ao Marketing - Curso de Marketing*. Sebenta, Leiria, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

MAGALHÃES, F.; PEREIRA, M. (2018), *Regulamento Geral de Proteção de Dados. Manual Prático* (2.ª ed.), Porto, Vida Económica.

MARQUES, E.; MEIRELES, J. (2018), *Privacidade Eletrónica: da diretiva à proposta de regulamento*, [Consult. a 20/05/2021]. Disponível em: https://www.publico.pt/2018/01/28/sociedade/opiniao/privacidade-eletronica-dadiretiva-a-proposta-de-regulamento-1801069

PEDREIRA, F. (2019), *Nova Lei do RGPD: "Agora é que vão começar os problemas jurídicos"*, [Consult. a 20/05/2021]. Disponível em: https://eco.sapo.pt/2019/09/26/nova-lei-do-rgpd-agora-e-que-vao-comecar-os-problemas-juridicos/

PORTAL DO DPO, *Encarregado de Proteção de Dados*, [Consult. a 17/05/2021]. Disponível em: https://www.portaldodpo.pt/blog/service/cookies/

REGENTE, D. (2015), *A proteção de dados pessoais e privacidade do utilizador no âmbito das comunicações eletrónicas*, Trabalho Final de Mestrado em Direito, Lisboa, Universidade Autónoma de Lisboa.

RIBEIRO, F. (2017), *O Tratamento de Dados Pessoais de Clientes para Marketing, Trabalho Final de Mestrado em Direito*, Lisboa, Universidade Autónoma de Lisboa.

SANTOS, A. (2017), *As Diretivas Comunitárias de Proteção de Dados Pessoais e a sua Aplicação em Portugal: Barreiras e Facilitadores*, Trabalho Final de Mestrado em Gestão e Políticas Públicas, Lisboa, Universidade de Lisboa.

UNIÃO EUROPEIA, [Consult. a 17/05/2021]. Disponível em: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm