O Impacto do Regulamento Geral de Proteção de Dados nas Organizações: um Novo Paradigma
Tiago Moreira
ISCAC | 2018

Instituto Politécnico de Coimbra

Instituto Superior de Contabilidade e Administração de Coimbra

Tiago Filipe Monteiro Moreira

O IMPACTO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS NAS ORGANIZAÇÕES: UM NOVO PARADIGMA

Coimbra, maio de 2018

INSTITUTO POLITÉCNICO DE COIMBRA

INSTITUTO SUPERIOR DE CONTABILIDADE

E ADMINISTRAÇÃO DE COIMBRA

Tiago Filipe Monteiro Moreira

O Impacto do Regulamento Geral da Proteção de Dados Pessoais nas Organizações: Um Novo Paradigma

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Solicitadoria, sob a orientação do Professor Armando Veiga.

Coimbra, maio de 2018

TERMO DE RESPONSABILIDADE

Declaro ser o autor desta dissertação, que constitui um trabalho original e inédito, e que nunca foi submetido a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação.

Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação.

Seguindo as normas institucionais do Instituto Politécnico de Coimbra e consequentemente do Instituto Superior de Contabilidade e Administração de Coimbra para a elaboração de uma dissertação, ter-se-á em conta na sua redação, a norma portuguesa ISO 405 (NP ISO 405) que transposta e harmoniza a norma internacional ISO 690:2010 na estrutura predefinida e estandardizada quanto às regras de formatação e citação.

PENSAMENTO

"Com as redes sociais, a computação em nuvem, os serviços baseados na localização geográfica do utilizador e os cartões inteligentes, deixamos vestígios digitais em tudo o que fazemos. Neste «admirável mundo novo dos dados», necessitamos de um sólido conjunto de regras."

Comissão Europeia, 2012

DEDICATÓRIA

Dedico, esta dissertação a todos os que estiveram presentes nesta importante etapa da minha vida. Aos meus pais. Aos meus avós. Á minha irmã. Á minha namorada. Ao meu orientador.

AGRADECIMENTOS

Aos meus pais, pela compreensão e apoio incondicional.

À minha irmã, Silvia, pela ajuda.

Aos meus avós, Joaquina e João, pelo carinho e afeto.

À minha namorada e companheira, Susana, por estar sempre ao meu lado e pelo seu apoio em todos os momentos.

Aos meus colegas, que fizeram parte do meu percurso académico, especialmente os meus amigos por estarem sempre disponíveis em dar a sua opinião crítica.

À Dina e Francisco, que me acolheram em sua casa, facilitando as inúmeras deslocações entre Fornos de Algodres e Coimbra.

Ao meu orientador Professor Armando Veiga, por todo o seu apoio, conhecimento e disponibilidade prestada durante a realização da dissertação.

RESUMO

A escolha deste tema surge no âmbito do novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, ou mais comummente conhecido por Regulamento Geral sobre a Proteção de Dados. Este regulamento vem alterar profundamente as organizações no que respeita ao tratamento dos dados pessoais dos titulares, sejam eles clientes, fornecedores, trabalhadores ou administradores e gestores.

Assim, sendo pertinente uma adaptação à nova exigência da União Europeia a todos os Estados-Membros, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e livre circulação desses dados, e que revoga a Diretiva 95/46/CE, as organizações têm até 25 de maio de 2018 para se adaptar às novas obrigações e procedimentos.

É neste contexto que a escolha do tema se justifica, por ser um tema extremamente atual, em que as organizações se irão deparar com novos desafios sendo necessário uma rápida adaptação e interiorização.

Pelo que, se entende que as organizações, devem colocar na agenda todas as dúvidas que possam suscitar, e que permita chegar à data e estarem preparadas para este novo paradigma e evitem a aplicação de coimas pelo incumprimento das normas do regulamento. Como também, por ser um tema tratado na parte letiva do mestrado, e ter suscitado um interesse pessoal relativamente ao novo paradigma no tratamento de dados pessoais.

Palavras-chave: regulamento; dados pessoais; encarregado de proteção de dados; informação; acesso; direito ao apagamento.

ABSTRACT

The choice of this topic arises under the new Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016, or more commonly known as the General Data Protection Regulation. This regulation which profoundly changes the management of the personal data of the holders, whether customers, suppliers, employees or administrators and managers.

Accordingly, adapting to the new demand from European Union to all member states, on the protection of individuals with regard about the processing of personal data and the free movement of such data and repealing Directive 95/46/EC, organizations have until May 25th, 2018 to adapt to new obligations and procedures.

It is in this context that the choice of topic is justified, since it is an extremely current topic, in which organizations will encounter new challenges, requiring rapid adaptation and internalization.

So, it is understood that organizations, should put on the agenda all doubts that may arise, in which it allows to arrive at the date and be prepared for this new paradigm and avoid the application of fines for non-compliance with the rules of the regulation. As well as being a topic dealt with in the academic part of the master's degree and having aroused a personal interest in the new paradigm in the processing of personal data.

Keywords: regulation; personal data; data protection officer; information; access; right to be forgotten.

ÍNDICE GERAL

LISTA DE ACRÓNIMOS, SIGLAS E ABREVIATURAS

ACI	Autoridade de Controlo Independente
ACP	Autoridade de Controlo Principal
AEPD	Agência Espanhola de Proteção de Dados
AIPD	Avaliações de Impacto sobre a Proteção de Dados
al.	Alínea
ANHPD	Autoridade Nacional Húngara para a Proteção de Dados
art.º	Artigo
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CE	Comissão Europeia
CEPD	Comité Europeu para a Proteção de Dados
Cit.	Citação n.º
CNPD	Comissão Nacional da Proteção de Dados
CRP	Constituição da República Portuguesa
D95	Diretiva 95/46/CE
EPD	Encarregado de Proteção de Dados
EUA	Estados Unidos da América
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
GDPR	*General Data Protection Regulation*
ibid.	*Ibidem*
ISO	*International Organization for Standardization*
LPDP	Lei da Proteção dos Dados Pessoais
n.º	Número

n.os	Números
p.	Página
pp.	Páginas
RGPD	Regulamento Geral da Proteção de Dados
TFUE	Tratado sobre o Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
UE	União Europeia
vide	Veja-se em

INTRODUÇÃO

Em matéria de proteção de dados, a implementação de uma nova regulamentação no contexto europeu, surge através das comunicações COM (2010) 609 final e COM (2012) 11 final, pela Comissão Europeia (CE). [1]

Nas referidas comunicações, em matéria de proteção de dados pessoais, há o levantamento de questões pertinentes, no que concerne à evolução tecnológica, à consequente globalização, ao melhoramento no processo de transferência de dados pessoais e a necessidade de haver um aprofundamento normativo, na proteção adequada aos titulares de dados pessoais.

No ordenamento jurídico português, o direito à vida privada pertence ao capítulo dos direitos fundamentais consagrados na Constituição da República Portuguesa (CRP). O direito à reserva sobre a intimidade da vida privada e o direito à utilização da informática estão consagrados nos Direitos, Liberdades e Garantias, respetivamente, nos artigos 26.º, n.º 1 e 35.º da (CRP).

Este direito fundamental surge, nos dias de hoje, com mais enfase do que nunca. Trata-se de uma mudança ou mais necessariamente, um reforço de mentalidades, devido à rápida evolução tecnológica e da consequente globalização. O aparecimento das redes sociais, e de todas as aplicações informáticas, a ideia de invasão aos nossos dados pessoais, surge como um novo desafio em matéria de proteção de dados pessoais no contexto jurídico-legal. [2]

O direito à proteção de dados surge devido à conflitualidade de interesses entre os cidadãos e o Estado. No contexto europeu, devido à aplicação direta das normas europeias, todos os Estados-Membros, estão sujeitos aos textos legais da União Europeia (UE), ou seja, prevalecem sobre as leis nacionais. É neste sentido que o Regulamento Geral de Proteção de Dados (RGPD), o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, surge para criar uma proteção mais sólida no panorama do cidadão europeu em matéria de dados pessoais.

O verdadeiro impacto do RGPD surge nas organizações, é este o "*novo paradigma*" relativamente aos dados pessoais. As novas práticas a implementar, o reforço das regras e a

[1] CE. (2010). COM (2010) 609 final. *Uma abordagem global da proteção de dados pessoais na União Europeia*. Acedido em 08 de janeiro de 2018. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0609:FIN.

CE. (2012). COM (2012) 11 final. *Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Acedido em 08 de janeiro de 2018. Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN.

[2] Considerando (6) e (7) do RGPD.

constante necessidade de salvaguardar a proteção dos titulares de dados pessoais que estejam ligados à organização.

Assim, as organizações estabelecidas em território da UE, e aquelas que estejam localizadas fora da UE, mas que tratem dados de pessoais de titulares aí residentes, devem estar preparadas para este panorama legal, e adotarem mecanismos que as possam acompanhar ao longo da sua atividade, de modo a evitar o incumprimento normativo e consequentes coimas. [3]

O tema da dissertação, compreende neste sentido, a implementação do RGPD nas organizações, e as alterações no sistema jurídico dos Estados-Membros. Inicialmente, será tratada a contextualização histórica da evolução da temática de proteção de dados pessoais na UE e em Portugal. Depois, a conceptualização dos princípios subjacentes à implementação do RGPD, e direitos do titulares de dados pessoais, que alteram o paradigma profundamente o meio organizacional, em tomar medidas efetivas no tratamento de dados pessoais. E por fim, as consequências do incumprimento do regulamento, no contexto de fiscalização pelas autoridades competentes.

O procedimento metodológico, consiste no método sistemático e dedutivo em analisar as normas do RGPD no tratamento de dados pessoais, com os direitos do titulares na proteção das liberdades e garantias dos mesmos, através da recolha de informação, nomeadamente legislação em vigor, jurisprudência, artigos científicos e publicações.

É com este novo panorama, que as organizações a par de todos os avanços tecnológicos, e na interação multinacional com todos os indivíduos que façam parte da estrutura organizacional, que novas medidas e sensibilização sobre a matéria de proteção de dados, deverá ser incutida na mentalidade de todos os envolventes para que não haja repercussões para a organização, mas fundamentalmente para o titular dos dados pessoais.

[3] Considerando (23) do RGPD.

CAPÍTULO I – O RGPD: CONSIDERAÇÕES INICIAIS

1. Evolução do processo legislativo

A UE como união económica e política, de livre circulação de bens e pessoas entre os Estados-Membros, deve assegurar os direitos fundamentais constantes da Carta dos Direitos Fundamentais da União Europeia (CDFUE) de forma coerente. Na panóplia de direitos fundamentais inseridos nos artigos da CDFUE, e em virtude do tema escolhido, especialmente numa era de modernização, mudanças tecnológicas e afirmação do indivíduo enquanto cidadão de uma "*aldeia global informatizada*", é necessário assegurar em matéria de proteção de dados pessoais a aplicação da lei e prevenção da criminalidade.

Assim, contextualizando a base jurídica na prevenção da violação do direito à proteção de dados pessoais, o art.º 7.º e 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE), [4] [5] e o art.º 8.º da CDFUE. [6]

De referir, a Convenção 108 de 1981 do Conselho da Europa para a Proteção das Pessoas Singulares relativamente ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, sendo conhecido pelo primeiro instrumento internacional na proteção de dados pessoais.

Até dia 25 de maio de 2018, os documentos legais a nível europeu, em vigor, relativamente à proteção de dados pessoais, era Diretiva 95/46/CE (D95), quanto à privacidade, a Diretiva 2002/58/CE (alterada em 2009), a Diretiva 2006/24/CE relativa à conservação de dados, o Regulamento (CE) n.º 45/2001 relativo ao tratamento de dados pessoais por instituições e órgãos comunitários, a Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção de dados pessoais tratados no âmbito da cooperação

[4] Art.º 7.º do TFUE: *"Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."*

Art.º 16.º do TFUE: "*1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 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*."

[5] Considerando (1) e (12) do RGPD.

[6] Art.º 8.º da CDFUE: *"1. Todas as pessoas têm direito proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."*

policial e judiciária de matéria penal, que será posteriormente revogada pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Também de mencionar, o Grupo de Trabalho do Artigo 29.º para a Proteção de Dados (GT29) que emite recomendações e pareceres. É um órgão independente sobre proteção de dados e privacidade sendo constituído por representantes das autoridades nacionais dos Estados-Membros da UE. Este GT29 será substituído pelo Comité Europeu para a Proteção de Dados (CEPD), nos termos do RGPD. [7]

Contudo, e agora seguindo o tema para a dissertação, em 2018 haverá um aprofundamento normativo imposto pelo RGPD, que foi iniciado a 25 de janeiro de 2012, pela comunicação COM (2012) 11 final, pelo que após um período de propostas e negociações, em dezembro de 2015, o Parlamento Europeu e o Conselho chegaram a acordo, em que procederá numa reforma da legislação à proteção de dados pessoais.

No nosso quadro legislativo nacional, havendo a implementação do RGPD, a D95 é revogada, como também da legislação nacional, ou seja, a Lei n.º 67/98, de 26 de outubro (LPDP), pelo que Portugal terá de se adaptar às novas exigências e desafios propostos pelo regulamento, estando em análise, a Proposta de Lei n.º 120/XIII. [8]

De referenciar, a autoridade administrativa independente e competente com atribuição em Portugal, para controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados, a Comissão Nacional de Proteção de Dados (CNPD).

A introdução do RGPD no contexto europeu vem reforçar, a ideia que já existia antes. A ideia de que a matéria sobre a proteção de dados em todos os Estados-Membros, tem um papel cada vez mais importante no contexto jurídico-legal, e que necessitava de ser reformulada em alguns aspetos, dado todo o avanço tecnológico, no qual o titular de dados pessoais, terá a primazia sobre o seu direito fundamental á privacidade.

[7] GT29. Acedido em 14 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358.

[8] XXI Governo Constitucional de Portugal. (2018). *Proposta de Lei n.º 120/XIII*. Acedido em 14 de maio de 2018. Disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368.

2. O objetivo principal do RGPD

O implementar do RGPD, vem alterar substancialmente as organizações, em matéria de dados pessoais. Assim, o objetivo principal, não será o de dotar as organizações de ferramentas para se protegerem, mas sim, o de proteger todo e qualquer titular de dados pessoais.

Constitui-se para as organizações, o lançamento de novos desafios e regras relativas à proteção de dados pessoais, que já advinha do referido art.º 8.º da CDFUE. Pode dizer-se que o RGPD tem como objetivos principais: implementar nos Estados-Membros mecanismos legislativos aliados à contínua evolução tecnológica, aumentar a proteção dada a todos os titulares de dados pessoais às ameaças constantes e utilização indevida desses dados pelas organizações, e de complementar a iniciativa da UE relativamente ao Mercado Único Digital, no que promete ser uma novo mecanismo de oportunidades a todos os cidadãos europeus e Estados-Membros, desde que disponham das competências digitais necessárias. [9]

O regulamento, vem implementar sérias medidas, entre as quais se destacam, como já foi mencionado anteriormente:

1. Introdução de uma nova categoria de profissional, ligada especificamente ao tratamento de dados pessoais (EPD);
2. Aplicação de coimas pelo incumprimento das normas do regulamento;
3. Alargamento da aplicação territorial do regulamento a todas as organizações que tratem dados pessoais, tanto dentro da UE como fora desta;
4. Autorregulação, em que deixará de ser necessário o envio de notificações e consequentes autorizações para a Autoridade de Controlo Independente (ACI);
5. Obrigação de notificação de violação por parte da organização à ACI, como também ao titular de dados pessoais;
6. Constituição do direito ao consentimento, no que respeita à exigência na informação a prestar aos titulares dos dados.

No contexto nacional, a CNPD elaborou um plano de medidas para "preparar a aplicação do RGPD." As medidas que a autoridade nacional de proteção de dados, elenca são as seguintes:

[9] CE. (2018). *Mercado Único Digital.* Acedido em 15 de maio de 2018. Disponível em https://ec.europa.eu/commission/priorities/digital-single-market_pt#policy-areas.

1. *"Deve rever a informação que fornece aos titulares dos dados, por escrito ou por telefone, no âmbito da recolha de dados, seja esta realizada diretamente junto do titular ou não."*

2. *"Deve rever os procedimentos internos de garantia do exercício dos direitos dos titulares dos dados, atendendo a novas exigências específicas do regulamento neste domínio quanto à tramitação dos pedidos, em especial aos prazos máximos de resposta."*

3. *"Deve verificar a forma e circunstâncias em que foi obtido o consentimento dos titulares, quando este serve de base legal para o tratamento de dados pessoais."*

4. *"Deve avaliar a natureza dos tratamentos de dados efetuados, a fim de apurar quais os que se podem enquadrar no conceito de dados sensíveis, e consequentemente se aplicarem condições específicas para o seu tratamento, relativas à licitude do tratamento, aos direitos ou às decisões automatizadas."*

5. *"Deve documentar de forma detalhada todas as atividades relacionadas com o tratamento de dados pessoais, tanto as que resultam diretamente da obrigação de manter um registo como as relativas a outros procedimentos internos, de modo a que a organização esteja apta a demonstrar o cumprimento de todas as obrigações decorrentes do RGPD."*

6. *"Deve rever os contratos de subcontratação de serviços realizados no âmbito de tratamentos de dados pessoais para verificar se contêm todos os elementos exigidos pelo regulamento."*

7. *"Deve preparar a designação do encarregado de proteção de dados com a antecedência devida, até porque este poderá desempenhar um papel fulcral neste período de transição para garantir que a organização cumpre todas as obrigações legais desde o início da aplicação do regulamento."*

8. *"Deve rever as políticas e práticas da organização à luz das novas obrigações do regulamento, e adotar as medidas técnicas e organizativas adequadas e necessárias*

para assegurar e poder comprovar que todos os tratamentos de dados efetuados estão em conformidade com o RGPD a partir do momento da sua aplicação."

9. *"Deve avaliar rigorosamente o tipo de tratamentos de dados que tenha projetado realizar num futuro próximo, de modo a analisar a sua natureza e contexto e os potenciais riscos que possam comportar para os titulares dos dados, de modo a aplicar com eficácia os princípios da proteção de dados desde a conceção e por defeito."*

10. *"Deve adotar procedimentos internos e ao nível da subcontratação, se for o caso, para lidar com casos de violações de dados pessoais, designadamente na deteção, identificação e investigação das circunstâncias, medidas mitigadoras, circuitos da informação entre responsável e subcontratante, envolvimento do encarregado de proteção de dados e notificação à CNPD, atendendo aos prazos prescritos no regulamento."* [10]

Penso que o grande aspeto a ter em conta, será o grande desafio da implementação que o regulamento terá ao nível da organização. Ou seja, na estruturação dos dados pessoais dos titulares, e na gestão dos mesmos, o verdadeiro impacto do RGPD estará na abordagem que a organização terá a partir do dia 25 de maio de 2018, relativamente ao tratamento dos dados pessoais dos titulares.

O conceito de proteção de dados pessoais, que até então não era considerado imperativo, passou a ser no contexto jurídico-legal da organização, um assunto primordial, e com especial atenção. A necessidade de ter um EPD é fundamental neste processo de implementação do regulamento.

A proteção de dados pessoais, quer na sua dimensão física ou digital, requererá das organizações um reforço das medidas de proteção. Isto irá impor às organizações, quer multinacionais, quer pequenas e médias empresas um verdadeiro esforço, na monitorização dos fluxos de dados pessoais, controlo dos mesmos e o aumento do nível de alerta quantos aos riscos de privacidade.

[10] CNPD. (2018). *10 Medidas para preparar a aplicação do Regulamento Geral de Proteção de Dados.* Acedido em 29 de janeiro de 2018. Disponível em https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf.

3. Outras disposições

Com o RGPD, também outros textos legais estão ligados ao mesmo tema, nomeadamente: a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais e à livre circulação desses dados, e a Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, relativa à utilização dos dados dos registos de identificação dos passageiros para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. [11]

A D95, que representa tudo o que ainda é aplicável em matéria de dados pessoais, é revogada, passando a ser implementado em vigor o RGPD. [12]

A transposição da D95 levou à criação da Lei n.º 67/98, de 26 de outubro (LPDP), ainda em vigor até ao dia 25 de maio de 2018. Esta lei, veio implementar no ordenamento jurídico português toda a matéria relativamente ao tratamento de dados pessoais: âmbito de aplicação da lei, a criação da autoridade de controlo, CNPD, inseriu os conceitos de tratamento de dados sensíveis, interconexão de dados pessoais, transferência de dados pessoais condições de legitimidade e direitos dos titulares, e transpôs o direito de informação, acesso e retificação. [13]

No contexto da legislação portuguesa, vem consagrado no art.º 35.º da CRP, o princípio da autodeterminação informativa, como desenvolvimento da personalidade, sendo um dos pilares dos direitos fundamentais da nossa constituição. [14]

---

[11] Considerando (19) do RGPD.

[12] Considerando (3) e (9) do RGPD.

[13] Considerando (10) do RGPD.

[14] Art.º 35.º da CRP: *"1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei."*

Este direito, afirma-se como um direito do cidadão oponível ao Estado, no que concerne ao direito do indivíduo na proteção dos dados pessoais, na sua privacidade informacional.

Neste aspeto, a existência de uma entidade administrativa independente no ordenamento jurídico português, já referenciada anteriormente, a CNPD, visa essencialmente, estabelecer um equilíbrio na garantia da proteção dos titulares de direitos pessoais, em contraste ao uso dos mesmos pelo Estado e organizações.

Afirma-se assim, que o aumento significativo da recolha e partilha de dados, lança constantemente novos desafios em matéria de proteção de dados pessoais. Esta constante evolução, necessita de uma proteção mais coerente na UE, que como se pode observar, houve a necessidade de implementar um novo regulamento, com aplicação mais rigorosa das regras, de modo a criar a confiança necessária aos titulares de dados pessoais.

O conceito de dados pessoais, segundo o RGPD, sofreu algumas alterações relativamente ao disposto na D95, passando a ter uma definição de maior amplitude.

Ora vejamos, o conceito segundo a D95 e o RGPD, respetivamente:

> *"Dados pessoais: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social."* [15]

> *"Dados pessoais: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); 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, indentificadores por via eletrónica ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular."* [16]

[15] Art.º 2.º, al. a) da Diretiva 95/46/CE.
[16] Art.º 4.º, n.º 1 do RGPD.

Na primeira definição de dados pessoais, segundo a D95, não se fazia referência aos elementos de identificação da pessoa singular através de um identificador, podendo segundo o RGPD, a pessoa singular ser direta ou indiretamente identificada, como por exemplo, por "*um nome, um número de identificação, dados de localização, indentificadores por via eletrónica.*"

A inclusão do elemento específico de identidade genética, e alteração de identidade psíquica para mental. Este elemento específico de identidade genética deve-se aos progressos observados na biotecnologia.

Por fim, as normas ISO (*International Organization for Standardization)*, ou normas de Organização Internacional para Padronização**,** em português. [17]

Nas diversas normas ISO, em matéria de proteção de dados pessoais e sistemas de gestão de segurança, destacam-se as seguintes:

1. A ISO/IEC 29100:2011 fornece um quadro de privacidade em que "e*specifica a terminologia de privacidade; define os atores e seus principais papéis em processar informações pessoalmente identificáveis; descreve considerações de salvaguardar a privacidade; e, fornece referencias a princípios de privacidade conhecidos para tecnologia da informação*." [18]

2. A ISO/IEC 29134:2017 que fornece um guia para "*processar avaliações de impacto de privacidade; e, estruturar e um relatório de avaliações de impacto*." [19]

3. A ISO/IEC 27005:2011 em que "*define as linhas de orientação e suporte na gestão de riscos de segurança da informação*." [20]

[17] A ISO é uma entidade de padronização e normatização, criada na Suíça, em 1947. A ISO tem como objetivo principal realizar o trabalho de definir, divulgar e aprovar normas técnicas. Acedido em 26 de maio de 2016. Disponível em https://www.iso.org/standards.html.

[18] A ISO/IEC 29100:2011 é "*aplicável a pessoas singulares e organizações envolvidas na especificação, aquisição, arquitetura, projeto, desenvolvimento, teste, manutenção, administração e operação de sistemas ou serviços de tecnologia da informação e comunicação onde são necessários controles de privacidade*." Acedido em 26 de maio de 2016. Disponível em https://www.iso.org/standard/45123.html.

[19] A ISO/IEC 29134:2017 é "*relevante para os envolvidos no projeto ou implementação de projetos, incluindo os sistemas operacionais de processamento de dados das partes e serviços*." Acedido em 26 de maio de 2016. Disponível em https://www.iso.org/standard/62289.html.

[20] A ISO/IEC 27005:2011 é "*aplicável a todos os tipos de organizações que pretendem gerenciar riscos que possam comprometer a segurança da informação da organização. Esta norma auxilia no cumprimentos dos requisitos especificados na norma ISO/IEC 27001 e foi desenhada para suportar a implementação eficaz de segurança da informação numa organização tendo por base a aproximação à gestão de riscos*." Acedido em 26 de maio de 2016. Disponível em https://www.iso.org/standard/56742.html.

4. A ISO/IEC 27001:2013 que "*especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação dentro do contexto da organização*." [21]

As normas ISO, visam essencialmente, dar certificação às organizações, na prossecução da garantia de que cumprem as mesmas, assegurando aos seus utilizadores de que, na situação em análise, a proteção dada ao tratamento de dados pessoais e às medidas de segurança na gestão dos riscos e avaliações de impacto, estão devidamente garantidas em consonância com o RGPD e os padrões de qualidade necessários, para determinar a confiança do titular de dados pessoais, no tratamento dado pela organização.

[21] A ISO/IEC 27005:2011 "*pode demonstrar a clientes, fornecedores e acionistas a integridade dos seus dados e sistemas, além de seu compromisso com a segurança da informação. A certificação do seu sistema de informação também pode levar a novas oportunidades de negócios com clientes preocupados com segurança, fortalecer a noção de sigilo em todo o local de trabalho e aumentar a ética dos funcionários. A certificação também permite que fortaleça a segurança da informação e reduza possíveis riscos de fraude, perda de informação e quebra de confidencialidade*." Acedido em 26 de maio de 2016. Disponível em https://www.iso.org/standard/54534.html.

CAPÍTULO II – OS PRINCÍPIOS SUBJACENTES AO TRATAMENTO DE DADOS PESSOAIS

1. Princípio da licitude, lealdade e transparência

No leque de princípios que já existiam, derivados da D95, houve um reforço e implementação de novos princípios que foram instituídos pelo RGPD.

O princípio da licitude, lealdade e transparência, conforme refere o art.º 5, n.º 1, al. a) do RGPD, diz que os dados pessoais são:

> *"Objeto de um tratamento lícito, leal e transparente em relação aos titulares dos dados."*

Os dados pessoais devem ser tratados licitamente, ou seja, *"deverão ser tratados com base no consentimento do titular dos dados em causa."* Este conceito de consentimento, como irá ser tratado na secção 8 deste capítulo, é o mais importante neste conjunto de princípios do RGPD. [22]

Quando ao princípio da lealdade, o tratamento dos dados pessoais, deve ser de forma leal, ou seja, de acordo com o fim a que se destinam e não outro, fortalecendo a ligação entre a organização e o titular dos dados pessoais, ficando este último consciente de que os seus dados serão utilizados, compreendidos e salvaguardados pela entidade que os recolheu.

O princípio da transparência, refere-se à certeza imediata do titular de dados pessoais, no que diz respeito, à recolha, utilização e consulta na medida em que os dados pessoais, serão tratados pela organização, este princípio "*... diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhe dizem respeito que estão a ser tratados.*" [23]

[22] Considerando (40) do RGPD.
[23] Considerando (39), (58) e (59) do RGPD.

2. Princípio da limitação das finalidades

O princípio da limitação das finalidades, segundo o art.º 5.º, n.º 1, al. b) do RGPD, refere-se que os dados pessoais são:

> *"Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo 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."*

Neste princípio, a recolha dos dados, não deve ser utilizada para fim diferente daquele que inicialmente foi recolhido. Ou seja, o titular de dados pessoais, ao fornecer os seus dados, tem a plena consciência de que o tratamento irá ser de acordo com a finalidade inicial. [24]

3. Princípio da minimização dos dados

O princípio da minimização dos dados, explica-nos o art.º 5.º, n.º 1, al. c) do RGPD, que os dados pessoais são:

> *"Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados."*

Quanto ao princípio da minimização dos dados, estes ao serem recolhidos pela organização, devem ser especificamente limitados ao fim a que se destinam, não podendo ser usados para outro fim, ao qual o titular de dados pessoais não tenha consentido. [25]

O tratamento de dados pessoais para outros fins, deverá como foi dito, ser autorizado pelo titular dos mesmos dados, de modo a assegurar a proteção necessária e a confidencialidade dos dados pessoais conservados.

[24] Considerando (39) do RGPD.
[25] Considerando (39) e (50) do RGPD.

4. Princípio da exatidão

O princípio da exatidão, conforme enuncia o art.º 5.º, n.º 1, al. d) do RGPD, que os dados pessoais são:

> *"Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora."*

As medidas adequadas a que se refere o artigo em questão, levam a que o responsável pelo tratamento de dados, quando exigido pelo titular desses dados pessoais, ter no imediato as ferramentas necessárias para a prossecução do cumprimento da exatidão e atualização dos dados inexatos. Como também a sua eliminação, ou retificação num prazo razoável, sem demora. [26]

5. Princípio da limitação da conservação

O princípio da limitação da conservação, segundo o art.º 5.º, n.º 1, al. e) do RGPD, que os dados pessoais são:

> *"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 pessoais podem 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 presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados."*

[26] Considerando (39) do RGPD.

Os dados pessoais "*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.*"

Ou seja, até aqui, a prática comum das organizações, relativamente aos dados pessoais que recolhiam, seriam de certo modo, conservados por tempo indeterminado, ou até mesmo reproduzidos, para fins diferentes da suposta recolha inicial.

Com o RGPD há uma mudança de paradigma quanto a este princípio. Ou seja, como foi dito anteriormente, os dados são recolhidos e limitados ao fim a que se destinam. No entanto, devem ser tratados até ao termo do período necessário para esse mesmo fim, exceto, a sua conservação poderá ser mais prolongada, se observar-se o disposto no art.º 5, n.1, al. e), *in fine* do RGPD. [27]

6. Princípio da integridade e confidencialidade

O princípio da integridade e confidencialidade, segundo o art.º 5.º, n.º 1, al. f) do RGPD, que os dados pessoais são:

> *"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, adotando as medidas técnicas ou organizativas adequadas."*

As medidas a adotar pela organização, de modo a implementar nas práticas de boa utilização dos dados pessoais dos titulares, devem obedecer ao princípio da integridade e confidencialidade.

Ou seja, a organização deve adotar medidas de proteção, que garantam a segurança dos dados pessoais contra possíveis invasões. Certamente nesta medida, tanto surgirá a proteção em termos físicos como digitais. Físicos de modo a que não estejam ao alcance de quem não é legitimamente responsável pelo tratamento dos dados, como a proteção digital, segundo a aplicação de um sistema informático capaz de combater as "*ações maliciosas ou ilícitas que*

[27] Considerando (39) e (50) do RGPD.

comprometam a disponibilidade, autenticidade, integridade e a confidencialidade dos dados pessoais conservados." [28]

7. Princípio da responsabilidade

O princípio da responsabilidade, enuncia o art.º 5.º, n.º 2 do RGPD, que o responsável pelo tratamento de dados:

> *"O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo."*

O responsável pelo tratamento de dados, deve assegurar o cumprimento de todos os princípios enunciados anteriormente. [29]

Esta responsabilidade aplica-se tanto ao responsável pelo tratamento como ao subcontratante, como se irá observar no Capítulo V.

O responsável pelo tratamento, segundo o art.º 4.º, n.º 7 do RGPD entende-se 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; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro."*

O subcontratante, define o art.º 4.º, n.º 8 do RGPD que:

> *"Uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes."*

[28] Considerando (39) e (49) do RGPD.
[29] Considerando (24), (47) e (48) do RGPD.

Estas duas aceções, quanto ao responsável pelo tratamento de dados, e o subcontratante, já advinham da D95. No entanto, o RGPD vem reforçar os deveres relativos ao subcontratante, nomeadamente quanto ao incumprimento das regras de proteção de dados pessoais. [30]

8. Princípio do consentimento

O conceito do consentimento, de acordo, com o art.º 4.º, n.º 11 do RGPD, define:

> *"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."*

Ou seja, tal como na D95, o consentimento surge no RGPD como o principal fundamento de legitimidade do tratamento de dados pessoais, em que é exigido "*mediante declaração ou ato positivo inequívoco*" que os dados pessoais, ao serem tratados "*dizem respeito*" ao titular desses mesmos dados. [31]

O princípio do consentimento, resulta do art.º 7.º do RGPD, em que se estabelecem as condições de legitimidade para validar o tratamento dos dados pessoais.

As condições quanto ao consentimento, referem que o "*responsável pelo tratamento deve demonstrar que o titular dos dados pessoais deu o seu consentimento*." Ou seja, é necessário, quando for exigido ao responsável pelo tratamento, deve comprovar o consentimento dado pelo titular, de forma a corroborar a intenção do mesmo. [32]

"*O consentimento dado em declaração escrita relativo a outros assuntos, deve ser apresentada de modo inteligível, fácil acesso e numa linguagem clara e simples*." Quanto ao consentimento que seja dado com consentimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento de dados e as finalidades a que esse tratamento se destina. Não deverá constituir consentimento, o silêncio, as opções pré-validadas ou a omissão. [33]

[30] Considerando (74), (79) e (81) do RGPD.
[31] Considerando (32), (42), (43) e (50) do RGPD.
[32] Art.º 7.º, n.º 1 do RGPD.
[33] Art.º 7.º, n.º 2 do RGPD.

"*O titular dos dados pessoais tem o direito de retirar o consentimento a qualquer momento.*" Esta situação tornas as organizações obrigadas a remover o consentimento pela mesma forma como foi concedido, ou seja, através da plataforma em que inicialmente foi tratado, quer seja por correio eletrónico, ou no sítio da internet, entre outros. [34]

O consentimento "*é dado livremente, e há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato*." [35]

Também, quanto às condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade de informação, estabelece o art.º 8.º do RGPD, este só é lícito se tiver pelo menos 16 anos de idade. Os Estados-Membros podem alterar a idade permitida para prestar o consentimento, desde que "*... essa idade não seja inferior a 13 anos de idade.*" [36]

Esta é uma realidade cada vez mais comum, ou seja, a prestação do consentimento para o tratamento de dados pessoais, deve estar presente até nas simples transações comerciais que o titular de dados pessoais faça, quer presencialmente quer através de um sítio na internet.

O conceito de consentimento deve ser alargado às instituições públicas, nomeadamente na área da saúde, e no caso das crianças, no âmbito escolar, e em particular nas atividades extracurriculares, em que as mesmas estão sujeitas ao descontrolo desenfreado da utilização dos dados pessoais. Deste modo, as crianças, ao longo do RGPD, pode-se observar que "*merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais*." [37]

Outro assunto, de especial interesse, ainda no âmbito do consentimento, é o tratamento de dados pessoais de sensíveis. [38]

Estes merecem, especial proteção específica, enuncia o art.º 9.º, n.º 1 do RGPD:

> "*É proibido o tratamento de 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, dados biométricos*

[34] Art.º 7.º, n.º 3 do RGPD.
[35] Art.º 7.º, n.º 4 do RGPD.
[36] Art.º 8.º, n.º 1 do RGPD.
[37] Considerando (38) do RGPD.
[38] Considerando (51), (52) e (53) do RGPD.

> *para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa*."

Segundo a D95, este conceito de dados sensíveis, já era tratado de forma especial, enunciado como dados sensíveis aqueles que "… *revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual*."

Ou seja, o leque de dados sensíveis, com a implementação do RGPD passou a ter uma maior amplitude, no que diz respeito ao "*tratamento de dados genéticos*", aos "*dados biométricos para identificar uma pessoa de forma inequívoca*" e o reforço dos dados ligados à vida sexual, em que se faz referência à "*orientação sexual de uma pessoa.*"

No entanto, esta categoria de dados, pode ser objeto de tratamento, desde que o seu fim, seja relacionado com a saúde, quando tal for necessário, "*para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo*."

O GT29, elaborou um conjunto de orientações sobre o princípio do consentimento. [39]

Nas orientações recomendadas, o GT29 afirma a verdadeira responsabilidade no tratamento de dados pessoais, em que a "*obrigação está nos controladores em inovar para encontrar novas soluções que operem dentro do parâmetros da lei e assegurar a proteção dos dados pessoais e os interesses dos sujeitos*." [40]

O princípio do consentimento, é de facto, uma grande alteração em matéria de tratamento de dados pessoais. O RGPD, vem obrigar as organizações no sentido de que, o titular de dados pessoais, deve ser informado do fim a que se destinam a recolha dos seus dados, mas para que isso tal aconteça, o tratamento deve ser consentido de "*forma gratuita, específica, informada e mediante declaração ou ato positivo inequívoco.*" [41]

[39] GT29. (2016). *Guidelines on consent under Regulation 2016/679. WP 259 rev.01.* Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051.
[40] *ibid.* GT29. (2016). Cit. 39. p. 3.
[41] *ibid.* GT29. (2016). Cit. 39. pp. 5-20.

CAPÍTULO III – O ÂMBITO DE APLICAÇÃO DO RGPD

1. Aplicação territorial

No âmbito da aplicação territorial, o RGPD aplica-se "*ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.*" [42]

É certo, que o RGPD, dada a sua dimensão de aplicação, este abrange todas as organizações que estejam instaladas na UE, e fora desta, se o tratamento dos dados pessoais, como enuncia o art.º 3.º, n.º 1 do RGPD, fora da UE. [43]

Refere o n.º 2 do mesmo artigo, que o RGPD se aplica não só "*ao contexto das atividades de um estabelecimento responsável pelo tratamento ou de um subcontratante*," como também "*ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante.*"

No aspeto, do tratamento de dados de titulares de residentes na UE, apenas se aplica o RGPD se as atividades de tratamento estiverem relacionadas com: "*a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares de dados procederem a um pagamento,*" e "o *controlo do seu comportamento, desde que esse comportamento tenha lugar na União*."

Ou seja, mesmo que uma organização não esteja situada territorialmente na UE, mas que cuja atividade esteja direcionada para os consumidores residentes na UE, esta organização estará sujeita ao RGPD, nomeadamente as atividades direcionadas a sítios na internet.

Este alargamento do âmbito de aplicação territorial, conduz a que o tratamento seja mais equilibrado entre os responsáveis pelo tratamento de dados situados dentro e fora da UE.

2. Aplicação material

Quanto ao âmbito de aplicação material, o art.º 2.º, n.º 1 do RGPD, refere que o mesmo regulamento "*aplica-se ao tratamento de dados pessoais por meios total ou parcialmente*

[42] Art.º 3.º, n.º 1 do RGPD.
[43] Considerando (22), (23), (24) e (25) do RGPD.

automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados."

Neste sentido, o RGPD aplica-se a todas as formas de tratamento de dados pessoais, mesmo automatizadas. Ou seja, as organizações que realizem operações que envolvam dados pessoais, ficam abrangidas em razão de matéria, mesmo que o tratamento desses dados, seja "*total ou parcialmente automatizados*" e "*não automatizados.*"

Por automatização de dados pessoais, entende-se como o processo em que a organização otimiza, a recolha e tratamento, com o objetivo de reduzir o esforço associado, e permitir executar as atividades relacionadas com os mesmos, em aplicações digitais, substituindo os processos manuais. Este processo de automatização resulta em maior eficácia na otimização, monitorização e controlo por parte da organização.

CAPÍTULO IV – OS DIREITOS DO TITULAR DOS DADOS

1. Transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados

Conforme foi dito, o princípio da transparência "*refere-se à certeza imediata do titular de dados pessoais, no que diz respeito, à recolha, utilização e consulta na medida em que os dados pessoais, serão tratados pela organização.*" [44]

Segundo o art.º 12.º do RGPD, vem elencado a transparência e regras para o exercício dos direitos dos titulares dos dados. Esta exigência, é naturalmente imputada ao responsável pelo tratamento dos dados pessoais e subcontratantes.

Entre as várias regras, o responsável que se identifica 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,*" tem o compromisso de:

1. *"Tomar as medidas adequadas para fornecer ao titular dos dados pessoais as informações e qualquer comunicação, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças;"*

2. *"Facilitar o exercício dos direitos do titular dos dados pessoais;"*

3. *"Fornecer ao titular as informações sobre as medidas tomadas, mediante pedido, sem demora injustificada e no prazo de um mês a contar da data da receção do pedido;"*

4. *"Informar sem demora, se não der seguimento ao pedido apresentado pelo titular dos dados, no prazo de um mês a contar da data da receção do pedido, das razões que o levaram a não tomar as medidas e da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial;"*

[44] Considerando (39), (58), (59) e (60) do RGPD.

5. *"Fornecer gratuitamente todas as informações quanto às comunicações e medidas tomadas. No entanto, tal pode ser afastado, e ser exigido o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações, e se os pedidos forem manifestamente infundados ou excessivos, pode recusar-se a dar seguimento ao pedido;"*

6. *"Solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados, quando houver dúvidas razoáveis quanto à identidade da pessoa singular que se apresenta;"*

7. *"Fornecer ao titular de dados pessoais, ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e legível, uma perspetiva geral significativa do tratamento previsto."* [45]

Para as organizações, poderem entender melhor o conceito de transparência no tratamento de dados pessoais, o GT29 elaborou um conjunto de orientações. [46]

De facto, a figura do responsável pelo tratamento de dados, deve assegurar a efetivação do cumprimento dos direitos do titular. Deste modo, o RGPD, veio estabelecer no responsável pelo tratamento de dados pessoais, a obrigação de atuar em conformidade com o regulamento, protegendo os interesses do titular de dados pessoais.

2. Direito de informação e acesso

O direito de informação do titular de dados pessoais, vem estipulado nos artigos 13.º e 14.º do RGPD, sendo as informações a facultar quando os dados são, ou não recolhidos junto do titular. [47]

O direito de acesso, refere-se ao direito do titular em aceder aos seus dados e obter do responsável pelo tratamento os dados pessoais que lhe digam respeito.

[45] Art.º 12.º do RGPD.
[46] GT29. (2016). *Guidelines on transparency under Regulation 2016/679. WP 260 rev.01*. Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[47] Considerando (61), (62) e (63) do RGPD.

No direito à informação junto do titular, segundo o art.º 13.º do RGPD vem elencadas as informações que o responsável pelo tratamento de dados deve facultar ao titular. [48]

Relativamente à informação que deve ser fornecida junto do titular, o Acórdão C-201/14, de 01 de outubro de 2015, do Tribunal de Justiça da União Europeia (TJUE), que opôs *Smaranda Bara* contra a *Agenţia Naţională de Administrare Fiscală* (Agência Nacional de Administração Fiscal da Roménia) e a *Casei Naţionale de Asigurări de Sănătate* (Casa Nacional de Segurança Social da Roménia), esclarece o direito à informação implementado pela D95.

Ou seja, foram comunicados dados pessoais entre as duas entidades romenas, sem que o titular dos dados pessoais em questão, *Smaranda Bara* tivesse consentido ou sequer sido previamente informado, quanto á legalidade da transmissão dos dados, relativamente aos rendimentos declarados para pagamento de contribuições em atraso para o regime de seguro de doença. Ora, conforme enuncia a D95, houve uma violação clara dos artigos 10.º, 11.º e 13.º da referida diretiva. [49]

Quanto às informações a facultar ao titular de dados, quando o responsável não está junto a este, o responsável deve fornecer as informações do art.º 14.º, n.º 1 do RGPD. [50]

---

[48] Art.º 13.º, n.º 1 do RGPD: *"a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas."*

[49] TJUE. (2015). Acórdão n.º C-201/14, de 01 de outubro de 2015. Acedido em 02 de fevereiro de 2018. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=168943&doclang= PT.

TJUE. (2015). Comunicado de Imprensa n.º 110/15, de 01 de outubro de 2015. Acedido em 02 de fevereiro de 2018. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110pt.pdf.

[50] Art.º 14.º, n.º 1 do RGPD: *"a) A identidade e os contatos do responsável pelo tratamento e, se for caso disso, do seu representante; b) Os contactos do encarregado da proteção de dados, se for caso disso; c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; d) As categorias dos dados pessoais em questão; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver; f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas."*

Ora, segundo o que já dispunha a D95, e agora o RGPD, o titular de dados pessoais, deve ser informado quanto ao tratamento dos seus dados, pelo que se não consentir, o responsável não deve utilizar esses dados para fim diferente daquele que inicialmente foram recolhidos.

Quanto ao direito de acesso do titular dos dados, o art.º 15.º do RGPD enuncia as situações caso haja tratamento dos dados que lhe digam respeito. [51]

O titular não deve ser impedido de forma alguma, de aceder aos dados a que lhe digam respeito. O acesso aos dados pessoais, deve ser fácil e gratuito. De mencionar, que caso os dados sejam transferidos para um país terceiro ou uma organização internacional, o titular deve ser informado das garantias adequadas.

No direito de acesso, o titular de dados pessoais, ao subscrever um produto financeiro, comercial ou de outra índole de interesse para o titular, este quando exercer o seu direito, deve obter do responsável pelo tratamento de dados, todas as situações de utilização desse produto que previamente subscreveu.

No entanto, este direito não é absoluto: "*o exercício do direito de acesso aos seus dados pessoais não deve afetar os direitos e as liberdades de outros, incluindo segredos comerciais ou propriedade intelectual.*" [52]

3. Direito de retificação

No direito de retificação, segundo o art.º 16.º do RGPD, o titular tem o direito de obter "*sem demora injustificada*", o acesso aos seus dados, para que o responsável pelo tratamento, possa atender ao pedido do titular de dados pessoais, para poder retificar os "*dados pessoais*

[51] Art.º 15.º, n.º 1 do RGPD: *"a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados."*

[52] CE. (2018). *Como posso aceder aos meus dados pessoais detidos por uma empresa/organização?* Acedido em 21 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisa tion_pt.

inexatos que lhe digam respeito." Esta retificação de dados inexatos deve ser acompanhada de uma declaração. [53]

Ou seja, o titular de dados pessoais, pode exercer o seu direito de retificação de dados pessoais, sendo essa retificação feita, no prazo de um mês. O tratamento dos dados pessoais, deve-se entender nesta situação, em que o titular dos mesmos, entenda que a informação detida pelo responsável, possa prejudicar em eventuais atos futuros para com outros, pela inexatidão ou falta de coerência nos dados que lhe diga respeito.

4. Direito ao apagamento dos dados (direito ao esquecimento)

A necessidade de alterar o paradigma, relativamente à sensibilização, quanto ao tratamento de dados pessoais na UE, iniciou-se com a Comunicação COM (2010) 609. Nesta comunicação da CE, o direito ao apagamento dos dados, ou o direito a ser esquecido, surge como "*o direito de as pessoas impedirem a continuação do tratamento dos respetivos dados e de os mesmo serem apagados quando deixarem de ser necessários para fins legítimos*."

O direito ao esquecimento, é um reforço do titular de dados pessoais no controlo dos seus dados e no próprio consentimento que este dá ao tratamento desses mesmos dados. [54]

Neste sentido o art.º 17.º do RGPD vem esclarecer o direito do titular de dados pessoais ao seu esquecimento. O titular tem o direito de "*obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos motivos*" explanados no n.º 1 do art.º 17.º do RGPD. [55]

Ou seja, o direito ao esquecimento, depende se o fim para o qual foram recolhidos os dados pessoais do titular, deixaram de ser objeto de tratamento dado atingirem a sua finalidade.

---

[53] Considerando (59) e (65) do RGPD.

[54] AUSLOOS, Jef. (2012). *The right to be forgotten – Worth remembering?* Computer Law & Security Review. Volume 28. Issue 2. pp. 143-152. Elsevier Ltd. Disponível em https://www.sciencedirect.com/science/article/1pii/S0267364912000246?via%3Dihub. doi: 10.1016/j.clsr.2012.01.006.

[55] Art.º 17.º, n.º 1 do RGPD: "*a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento; c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2; d) Os dados pessoais foram tratados ilicitamente; e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.*"

Também se aplica, caso os titulares "*retirem o seu consentimento ou se opuserem ao tratamento dos dados que lhe digam respeito, ou se o tratamento não respeitar o disposto no RGPD.*" [56]

Este é essencialmente, o principal direito do titular de dados pessoais, que vem consagrado no RGPD. Há uma alteração de paradigma, principalmente no tratamento a dar aos dados pessoais pelas organizações. Estas devem estar dotadas de mecanismos que atempadamente, possam eliminar os dados pessoais caso o titular assim deseje de modo a cumprir o disposto no regulamento.

A situação do direito ao esquecimento, surgiu com mais impacto na UE, e dotou os cidadãos europeus para um novo reconhecimento dos seus direitos, quanto ao tratamento a dar aos dados pessoais, quando estes atingem o seu propósito.

Em Espanha, o referido direito esteve em debate, em que opôs a *Google Spain* contra *Mario Costeja González* e *Agencia Española de Protección de Datos* (AEPD – Agência Espanhola de Proteção de Dados), no Acórdão C-131/12, de 13 de maio de 2014, do TJUE.

No referido caso, *Mario Costeja González* ao fazer uma pesquisa pelo seu nome no motor de busca *Google Spain*, reparou que "*a lista de resultados exibia ligações para duas páginas do jornal diário da La Vanguardia, ..., que anunciavam, ..., uma venda de imóveis em hasta pública organizada na sequência de um arresto destinado a cobrar as dívidas de Mario Costeja González à Segurança Social*." [57]

Ora, nesta situação a AEPD, ordenou à *Google Spain*, a "*adoção das medidas necessárias para retirar os dados do seu índice e impossibilitar o futuro acesso aos mesmos.*" Por entender que esses dados, poderiam ser acedidos por qualquer internauta, ao fazer uma pesquisa no motor de busca, sendo este o responsável pelo tratamento desses dados, dado que segundo a D95, é este que efetiva os fins e os meios pelo qual obteve os dados.

Neste sentido, o titular de dados pessoais, com a aplicação do RGPD, tem o direito ao apagamento dos seus dados, quando se atingir a finalidade pelo qual esses dados foram recolhidos pelo responsável.

Ou seja, a continuidade do tratamento de dados pessoais pelo responsável, à luz do RGPD, deve ser conservada, apenas durante o período necessário. As organizações, com a aplicação deste direito, devem estar dotadas de medidas técnicas e adequadas para satisfazer o

[56] Considerando (65) e (66) do RGPD.

[57] TJUE. (2015). Acórdão n.º C-131/12, de 13 de maio de 2014. Acedido em 04 de fevereiro de 2018. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang= PT.

TJUE. (2015). Comunicado de Imprensa n.º 70/14, de 13 de maio de 2014. Acedido em 04 de fevereiro de 2018. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pt.pdf.

titular de dados pessoais, e consequentemente obedecer aos termos legais do RGPD, relativamente ao direito ao esquecimento.

A configuração deste direito, não é de um direito absoluto, "*o que significa que outros direitos sejam também salvaguardados, como a liberdade de expressão e a investigação científica.*" [58]

5. Direito à limitação do tratamento

O titular de dados pessoais, tem o direito de obter do responsável pelo tratamento a limitação desse mesmo tratamento, se observar-se uma das situações do art.º 18.º, n.º 1 do RGPD. [59]

Ou seja, o titular pode exigir do responsável, que o tratamento dos seus dados pessoais, seja limitado aos seus interesses. Nesta situação, as organizações que estejam por lei, obrigadas a conservar os dados pessoais, o titular de dados pessoais, pode solicitar o exercício à limitação desses dados, para que não sejam utilizados para outros fins. [60]

6. Direito de portabilidade dos dados

O direito à portabilidade dos dados pessoais, vem estipulado no art.º 20.º do RGPD. O titular de dados pessoais, neste contexto, pode aceder aos seus dados e pedir que sejam transferidos para outro serviço, sempre que os dados pessoais sejam tratados de forma automatizada.

O titular de dados pessoais "*deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato*

---

[58] CE. (2018). *Posso pedir a uma empresa que apague os meus dados pessoais?* Acedido em 21 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-delete-my-personal-data_pt.

[59] Art.º 18.º, n.º 1 do RGPD: "*a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão; b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização; c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.*"

[60] Considerando (69) e (73) do RPGD.

estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável." [61]

Nesta situação, as organizações devem dotar-se de mecanismos interoperáveis que facilitem a portabilidade dos dados. Ao contrário da D95, que "*tinha como condicionante o formado escolhido pelo responsável pelo tratamento de dados para prestar as informações solicitadas*," o RGPD, "*permite dar mais poderes aos titulares de dos dados ..., dado que viabiliza a sua capacidade para transferir, copiar ou transmitir facilmente dados pessoais de um ambiente informático para outro.*" [62]

O GT29, refere as três condições cumulativas para a aplicabilidade deste direito. Em primeiro lugar, "*os dados pessoais solicitados devem ser tratados por meios automáticos, com base no consentimento prévio do titular dos dados.*" Em segundo lugar, "*os dados pessoais solicitados devem dizer respeito ao titular dos dados e ser fornecidos pelo mesmo.*" Por último, na terceira condição, "*o exercício deste novo direito não deve prejudicar os direitos e as liberdades de terceiros.*" [63]

O direito à portabilidade dos dados, anda a par com o avanço, nomeadamente das redes sociais. Neste contexto digital, em que a vida do cidadão, por opção deste, é cada vez mais configurada na livre escolha em colocar os seus dados nestas plataformas digitais, o titular de dados pessoais, vê com a aplicação do RGPD, neste novo direito, a faculdade de transportar os seus dados "*antes do encerramento de uma conta, a fim de permitir que o titular dos dados recupere e armazene os seus dados pessoais.*"

7. Direito de oposição e decisões individuais automatizadas (*profiling*)

Nos art.[os] 21.º e 22.º do RGPD, surge o direito de oposição e decisões individuais automatizadas.

O conceito de definição de perfis (*profiling*), segundo o art.º 4.º, n.º 4 do RGPD, é determinado como "*qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho*

[61] Considerando (68) do RPGD.
[62] GT29. (2016). *Orientações sobre o direito à portabilidade dos dados.* WP 242 rev.01. Acedido em 10 de fevereiro de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.
[63] GT29. (2016). *Perguntas Frequentes.* Anexo WP 242 rev.01. Acedido em 10 de fevereiro de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações."

O titular de dados pessoais, ao subscrever um produto, em que insira dados pessoais seus, tem "*o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.*" [64]

No entanto, o disposto no n.º 1 do art.º 22.º do RGPD quando ao processamento automatizado de dados pessoais, não se aplica segundo o constante das alíneas do n.º 2 do mesmo artigo. [65]

O levantamento de perfis, é uma prática comum no mundo organizacional. Deste modo, a aplicação do RGPD, vem estabelecer um novo paradigma quanto ao direito do titular de dados pessoais, no sentido de este se opor à sujeição do tratamento automatizado. Na subscrição de um produto, ou de um sítio da internet, com vista a compras on-line, o tratamento de dados pessoais, atualmente automatiza as escolhas do utilizador com base no seu perfil. No entanto, o titular de dados pessoais, após a implementação do RGPD, pode "*manifestar a sua opinião, contestar a decisão e solicitar que essa decisão tomada pelo algoritmo seja revista por uma pessoa.*" [66]

Quanto ao direito de oposição, segundo o art.º 21.º do RGPD, "*o titular de dados pessoais tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados, …, incluindo a definição de perfis.*"

O responsável pelo tratamento de dados, "*tem de assegurar que este direito de oposição, está explicito em qualquer documento ou sítio da internet e não escondido em qualquer parte dos termos e condições contratuais*." [67]

As condições em que o direito de se opor ao tratamento de dados pessoais, se os mesmos estiverem a ser tratados para as seguintes finalidades: "*comercialização direta; investigação*

---

[64] Art.º 22.º, n.º 1 do RPGD.

[65] Art.º 22.º, n.º 2 do RPGD: "*a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados*."

[66] GT29. (2017). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* WP 251 rev.01. Acedido em 21 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[67] *ibid*. GT29. (2017). Cit. 66.

científica/histórica e recolha de estatísticas; e, os seus próprios interesses legítimos ou para realizar uma tarefa do interesse público ou para uma autoridade pública." [68]

O titular de dados pessoais, ao contrário do que habitualmente se tem observado, após o RGPD, poderá cessar o tratamento dos dados pessoais, caso se observe alguma das condições referidas anteriormente, tendo em vista a finalidade de assegurar os interesses ou direitos e liberdades fundamentais do titular dos dados. [69]

[68] CE. (2018). *Posso pedir a uma empresa que cesse o tratamento dos meus dados?* Acedido em 21 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_pt.

[69] Considerando (69) e (70) do RGPD.

CAPÍTULO V – RESPONSABILIDADE PELO TRATAMENTO

1. A responsabilidade

Com a aplicação do RGPD, o responsável pelo tratamento de dados, no contexto organizacional, deve tomar medidas de modo a que as regras do referido regulamento, sejam aplicadas. Essas medidas organizativas, "*devem ser revistas e atualizadas consoante as necessidades.*"

No art.º 24.º do RGPD, está prevista a responsabilidade pelo tratamento de dados pessoais. Ou seja, o responsável pelo tratamento está obrigado a "*executar medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o RGPD*." [70]

O responsável pelo tratamento de dados, *vide* art.º 4.º, n.º 7 do RGPD, será aquela entidade na organização que deverá aplicar "*medidas técnicas e organizativas*" para assegurar o cumprimento de um nível de segurança quanto ao tratamento dos dados pessoais dos titulares.

As medidas, levam a que o responsável, possa garantir o nível de segurança desejado, dado que atinge todos os setores organizacionais, como por exemplo, no setor do *marketing*, tecnologias da informação, recursos humanos, administrativo, entre outros.

Neste sentido, o responsável, deverá analisar a situação da organização quanto aos processos que tratem dados pessoais, quais as medidas para adaptar o cumprimento do RGPD às necessidades da organização, como devem ser processados os dados pessoais, e assegurar de que esses dados, atingem um nível de segurança adequado.

Contudo, o responsável está obrigado a registar as atividades do tratamento, *vide* art.º 30.º, n.º 1 do RGPD, como também o seu subcontratante ou subcontratantes, *vide* n.º 2 do mesmo artigo. [71]

Sempre que houver tratamento de dados pessoais, o responsável, segundo o artigo mencionado anteriormente, deverá proceder e conservar a um registo pormenorizado, de qualquer ato que pratique, relativamente ao tratamento de dados pessoais. Para verificar esses registos, a ACI pode solicitar a disponibilização de todos esses atos. [72]

---

[70] Considerando (74) do RGPD.

[71] Considerando (82) do RGPD.

[72] Art.º 30.º, n.º 1 do RPGD: "*a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados; b) As finalidades do tratamento dos dados; c) A descrição das categorias de titulares de dados e das categorias de dados pessoais; d) As categorias de destinatários a quem os dados pessoais*

No entanto, o responsável para além das medidas mencionadas anteriormente, deve sensibilizar todos os setores que recolham dados pessoais, de modo a garantir que as normas sejam cumpridas. Ou seja, alterar o paradigma no que concerne à recolha de dados, que tão comummente se praticava, desde as fotocópias de dados pessoais, às divulgações nas redes sociais e às práticas dos funcionários nas organizações.

2. A proteção de dados pessoais desde a conceção (*Privacy by Design)* e por defeito (*Privacy by Default*)

Com a implementação do RGPD, é introduzido o conceito de proteção de dados pessoais desde a conceção e por defeito, embora esta matéria já estivesse presente na D95, agora com o RGPD, há um reforço deste conceito segundo o art.º 25.º do RGPD. [73]

Quanto à proteção de dados desde a conceção (*Privacy by Design*), o art.º 25.º, n.º 1 do RGPD menciona que "*tendo em conta as técnicas mais avançadas, ..., o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, ..., destinadas a aplicar com eficácia as garantias necessárias no tratamento*."

Ou seja, o responsável ao recolher os dados pessoais do titular, no momento, deve assegurar ao mesmo, que os seus dados são tratados de acordo com o regulamento, no cumprimento dos direitos do titular desde o início. [74]

A proteção de dados por defeito (*Privacy by Default*), o art.º 25.º, n.º 2 do RGPD, explica que "*o tratamento aplica medidas técnicas e organizativas para assegurar, ..., só sejam tratados os dados que forem necessários para cada finalidade específica de tratamento.*"

Neste conceito, o tratamento de dados pelo responsável, assegura ao titular de dados pessoais, que apenas recolhe os dados, que são necessários por um determinado período de

---

foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais; e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, a documentação que comprove a existência das garantias adequadas; f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados; g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 32.º, n.º 1."

[73] Considerando (78) do RGPD.

[74] CE. (2018). *O que significa a proteção de dados «desde a conceção» e «por defeito»?* Acedido em 22 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt.

conservação, ou acessibilidade limitada, "*para que não seja acessível a um número indefinido de pessoas*." [75]

É com efeito através do principio da minimização dos dados, que ao titular de dados pessoais, segundo as normas do RGPD que "*o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável,*" *vide* art.º 4.º, n.º 5 do RGPD.

Esta premissa, permite que em determinados processos de recolha de dados, estes dados, segundo o conceito de pseudonimização referido pelo artigo mencionado, sejam minimizados ou até mesmo apagados. [76]

De modo a obter uma proteção mais adequada no tratamento de dados pessoais, as organizações devem estar dotadas de mecanismos que impossibilitem a violação dos dados pessoais de ameaças externas, nomeadamente através da cifragem de dados. [77]

3. O subcontratante

A responsabilidade pelo tratamento de dados, é extensível ao subcontratado pelo responsável. O que resulta numa cadeia, quanto ao tratamento de dados pessoais, em que o titular de dados pessoais deve ter conhecimento de todos os responsáveis pelos seus dados.

Segundo o art.º 28.º, n.º 1 do RGPD, "*quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular de dados.*"

O subcontratante é, segundo o art.º 4.º, n.º 8 do RGPD, "*uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes*."

---

[75] CE. (2018). *O que significa a proteção de dados «desde a conceção» e «por defeito»?* Acedido em 22 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt.

[76] Considerando (26), (28) e (29) do RGPD.

[77] SAGE. (2018). *Guia prático da Sage para empresas.* Acedido em 29 de maio de 2018. Disponível em https://www.sage.pt/~/media/markets/pt/rgpd/images/GuiaPratico_GDPR.pdf.

Nesta situação o responsável pelo tratamento de dados, contratualiza com outro responsável subcontratado, para que trate os dados recolhidos junto do titular, e que assegure o mesmo nível de segurança e fiabilidade que o responsável.

Ou seja, em organizações com um elevado número de recolha de dados pessoais, como multinacionais, empresas financeiras ou até mesmo redes sociais, devem informar o titular de dados pessoais, que o tratamento é assegurado pelo responsável, como também, caso haja subcontratante, esse tratamento é igualmente fiável e de acordo com o cumprimento dos direitos do titular de dados pessoais. As mesmas regras se aplicam, caso o subcontratante não esteja na UE. [78]

4. A segurança do tratamento

Como já foi referido na Secção 3, do Capítulo em análise, a segurança do tratamento parte do responsável, que através de "*medidas técnicas e organizativas*" deverá assegurar, o cumprimento de um nível de segurança adequado, quanto ao tratamento dos dados pessoais dos titulares.

A violação de dados pessoais, é definida como "*uma violação da segurança que provoca, de modo acidental ou ilegal, a destruição, a perda, a alteração, a divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou de outro modo tratados no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público na Comunidade.*" [79]

No Parecer 03/2014, relativo à notificação da violação de dados pessoais, emitido pelo GT29, "*são fornecidas orientações aos responsáveis pelo tratamento, a fim de ajudá-los a decidir se devem ou não notificar as pessoas em causa, em caso de violação de dados pessoais*."

O GT29, estabelece as potenciais consequências e efeitos adversos da violação de dados pessoais, em casos que estejam em causa princípios, tais como: a confidencialidade, a disponibilidade e a integridade.

Assim, o RGPD prevê um reforço nas medidas a tomar em caso de violação de dados pessoais, que resultam na posterior notificação e comunicação dessa violação, tanto à ACI, como ao titular de dados pessoais. [80]

[78] Considerando (80) e (81) do RGPD.
[79] Art.º 2.º, al. i) da Diretiva 2002/58/CE.
[80] Art.º 33.º e 34.º do RGPD.

Segundo o art.º 33.º do RGPD, "*em caso de violação de dados, o responsável pelo tratamento de dados, notifica à autoridade de controlo competente, sem demora injustificada, e sempre que possível, até 72 horas após ter conhecimento da mesma, a menos que a violação dos dados pessoais seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.*"

Com a aplicação do RGPD, há uma obrigação que resulta na devida notificação à autoridade de controlo independente pelo responsável, sendo no caso português, a notificação à CNPD. [81]

Também, o responsável, segundo o art.º 34.º do RGPD, deve "*comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada*."

Assim, tanto a ACI como o titular de dados pessoais, são informados pelo responsável pelo tratamento de dados pessoais, em tempo imediato, acerca de qualquer violação que tenha ocorrido aos dados pessoais fornecidos. [82]

Nesta situação, podemos verificar o caso da *Uber*, "*empresa multinacional americana, que através de um aplicação digital, permite a busca por motoristas baseada na localização, oferecendo um serviço semelhante ao táxi tradicional*," relativamente à comunicação da violação de dados aos titulares de dados pessoais.

O caso da *Uber*, remonta a 2016 em que piratas informáticos, a troco de 100 milhões de euros para apagar os dados, roubaram informação a cerca de 57 milhões de utilizadores. A situação causou controvérsia, dado que a multinacional não informou os utilizadores da violação de dados, tais como o nome, correio eletrónico e contato telefónico. [83]

Para melhor entender o conteúdo normativo do RGPD, o GT29 elaborou um conjunto de orientações acerca de situações em que haja violação de dados pessoais. [84]

É com base, na evolução tecnológica e na facilidade de cada utilizador colocar os seus dados à disposição de aplicações digitais, entre outros produtos, que o RGPD veio reforçar este novo paradigma. Ou seja, os titulares de dados pessoais, estão cada vez mais conscientes para esta problemática, quanto à violação de dados pessoais, e as consequências que isso poderá ter nas suas vidas.

---

[81] Considerando (82) do RGPD.

[82] Considerando (86), (87), (88) e (89) do RGPD.

[83] The Guardian. (2017). *Uber concealed massive hack that exposed data of 57m users and drivers.* Acedido em 27 de maio de 2018. Disponível em https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

[84] GT29. (2017). *Guidelines on personal data breach notification under Regulation 2016/679.* WP 250 rev.01. Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

5. Encarregado de Proteção de Dados (*Data Protection Officer)*

A principal figura que o RGPD veio instituir nas organizações, é possivelmente o Encarregada de Proteção de Dados (EPD), ou seja o *Data Protection Officer (DPO)*, como internacionalmente é reconhecido.

Segundo o art.º 37.º do RGPD, as organizações devem nomear um EPD, sempre que: "*a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional; b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º*."

A respeito do EPD, o GT29 veio elaborar orientações específicas nesta matéria, em que esta figura deve agir em total autonomia, pertencendo ou não aos quadros da organização em que exerça as suas funções. [85]

As "*atividades principais*" podem entender-se como "*as operações essenciais para alcançar os objetivos do responsável pelo tratamento ou do subcontratante, as quais incluem também todas as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante*." [86]

O GT29 define "*grande escala*" dado que o RGPD não estipula o significado desse conceito, sendo que tal é entendido como "*o número de titulares de dados afetados, como número concreto ou em percentagem da população em causa; o volume de dados e/ou o alcance dos diferentes elementos de dados objeto de tratamento; a duração, ou permanência, da atividade de tratamento de dados; e, o âmbito geográfico da atividade de tratamento*." [87]

O "*controlo regular e sistemático*" pode entender-se como "*contínuo ou que ocorre a intervalos específicos num determinado período, recorrente ou repetido em horários estipulados, constante ou periódico, que ocorre de acordo com um sistema, predefinido,*

[85] GT29. (2016). *Orientações sobre os encarregados da proteção de dados (EPD).* WP 243 rev.01. Acedido em 22 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
[86] *ibid*. GT29. (2016). Cit. 85. p. 23.
[87] *ibid*. GT29. (2016). Cit. 85. p. 24.

organizado ou metódico, realizado no âmbito de um plano geral de recolha de dados, efetuado no âmbito de uma estratégia." [88]

Com a implementação do RGPD, surge uma nova categoria profissional, dedicada essencialmente ao tratamento de dados pessoais: "*Isso essencialmente cria uma profissão, talvez uma das várias novas profissões e carreiras relacionadas a questões de proteção de dados e o novo regime de proteção de dados. Isso enfatiza a nova importância atribuída aos dados pessoais.*" [89]

De referir, que no meio organizacional, a função do EPD não poderá resultar num conflito de interesses, ou seja, não poderá exercer funções que sejam da responsabilidade por quem procede ao tratamento de dados pessoais.

No sentido mais estrito, o EPD é quem tem competência para verificar se o RGPD está a ser escrupulosamente cumprido pelo responsável e subcontratante no tratamento de dados pessoais, no qual este, poderá aconselhar e recomendar medidas no tratamento desses dados, e recolher informações acerca das atividades do responsável e subcontratante.

A posição do EPD, demarca-se das funções do responsável e do subcontratante no que concerne ao tratamento de dados, embora apesar de estes, deverem cumprir o disposto no RGPD, o EPD também o deverá fazer, contudo, este último apenas coopera com a organização e com a ACI, no controlo sistemático do tratamento de dados pessoais.

Quanto à designação do EPD, o art.º 38.º do RGPD, reafirma a posição do EPD em demarcar-se da responsabilidade quanto ao tratamento de dados. Ou seja, esta responsabilidade pelo tratamento, cabe, como já se referiu ao responsável e ao subcontratante. Em caso de violação de dados pessoais, a organização não pode penalizar nem destituir o EPD das suas funções. [90]

As funções do encarregado da proteção de dados, surgem no art.º 39.º do RGPD: "*a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros; b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento*

[88] GT29. (2016). *Orientações sobre os encarregados da proteção de dados (EPD).* WP 243 rev.01. Acedido em 22 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. pp. 24-25.

[89] LAMBERT, Paul. (2017). *The Data Protection Officer*. First Edition. Taylor & Francis Group. p. 37.

[90] *ibid.* LAMBERT, Paul. (2017). Cit. 89. pp. 40-41.

ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º; d) Coopera com a autoridade de controlo; e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto."

Quanto às qualidades profissionais, o EPD "*deve se designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio das normas e práticas de proteção de dados, bem como na sua capacidade para desempenhar as respetivas funções*." [91]

As competências e conhecimentos especializados incluem: "*competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD, conhecimento das operações de tratamento efetuadas, conhecimento das tecnologias da informação e da segurança dos dados, conhecimento do setor empresarial e da organização, capacidade para promover uma cultura de proteção de dados no seio da organização*." [92]

Ou seja, o RGPD, veio definir que em matéria de proteção de dados, as organizações devem estar preparadas e nomear um EPD caso se verifique a obrigação de o ter. Contudo, as condições de nomear um EPD não são impeditivas de outras organizações, ou até mesmo em pequenas e médias empresas, de procurarem aconselhamento, junto de um EPD no que respeita ao tratamento de dados pessoais, podendo este ser contratado em regime de prestação de serviços.

6. As avaliações de impacto

As avaliações de impacto sobre a proteção de dados (AIPD), é um conceito que não está definido no RGPD. [93]

[91] GT29. (2016). *Orientações sobre os encarregados da proteção de dados (EPD).* WP 243 rev.01. Acedido em 22 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.
[92] *ibid*. GT29. (2016). Cit. 91. p. 26.
[93] GT29. (2016). *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE)*

Uma AIPD é "*um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos*." Por outras palavras, "*uma AIPD é um processo que visa estabelecer e demonstrar conformidade*." [94]

No art.º 35.º do RGPD é previsto que, quando houver um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento, antes de iniciar o tratamento, deve proceder a uma AIPD. [95]

No n.º 3 do referido artigo, o RGPD prevê alguns exemplos de quando é que é necessário realizar uma AIPD, nomeadamente: "*a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou c) Controlo sistemático de zonas acessíveis ao público em grande escala*."

Cabe ao responsável pelo tratamento de dados, introduzir na organização um guia que forneça as práticas relativamente ao tratamento de dados pessoais, desde que contemple o disposto no art.º 35.º, n.º 7 do RGPD.

Quando à metodologia a adotar, o RGPD não estabelece uma forma em particular. Contudo, as várias ACI dos Estados-Membros publicaram, diversas metodologias. [96]

Estas metodologias visam essencialmente, cumprir os critérios de forma exaustiva em conformidade com o RGPD. Sendo que a AIPD deve abranger pelo menos "*uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento*, *a necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, uma avaliação dos*

2016/679. WP 248 rev.01. Acedido em 22 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[94] GT29. (2016). *Orientações sobre os encarregados da proteção de dados (EPD).* WP 243 rev.01. Acedido em 22 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

[95] Considerando (90), (91), (92), (93) e (94) do RGPD.

[96] Por exemplo, o Modelo Normalizado de Proteção de Dados da Alemanha, disponível em https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/04/SDM-Methodology_V1_EN1.pdf; o Guia para uma Avaliação de Impacto na Proteção de Dados Pessoais da Espanha, disponível em https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf; e, o Código de Prática de Avaliações de Impacto de Privacidade do Reino Unido, disponível em https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

riscos para os direitos e liberdades dos titulares dos direitos, e as medidas previstas para fazer face ao discos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais." [97]

A implementação de uma AIPD na organização, é sobretudo agir em conformidade com o regulamento. Obtendo um planeamento ajustado que consiga assegurar um nível máximo de segurança no tratamento de dados pessoais dos titulares. Os critérios estipulados numa AIPD devem ser cumpridos, de modo a que resultem numa "*maior confiança por parte dos titulares dos dados para com os responsáveis pelo tratamento de dados e seus subcontratantes*." [98]

[97] Art.º 35.º, n.º 7 do RGPD.

[98] GT29. (2016). *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*. WP 248 rev.01. Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

CAPÍTULO VI – TRANSFERÊNCIA DE DADOS PESSOAIS

1. O princípio geral das transferências

Com a constante transferência de dados pessoais, em organizações internacionais, a responsabilidade pelo tratamento abrange não só os responsáveis pelo tratamento de dados pessoais e subcontratantes sediados na UE, como também aqueles que tratem dados fora da UE, estão abrangidos pelo RGPD. [99]

É neste contexto, que surge o princípio geral das transferências, segundo o art.º 44.º do RGPD. No referido artigo, enuncia-se que "*qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após a transferência para um país terceiro ou uma organização internacional, só é realizada se, sem prejuízo das outras disposições, ..., forem respeitadas pelo responsável pelo tratamento e pelo subcontratante*."

No entanto, a transferência de dados, para um país terceiro, deve observar a um nível adequado de proteção, "*garantindo a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro*." [100]

Relativamente a esta matéria, sobre o princípio da transferência de dados, foi amplamente debatida, no conhecido Acórdão C-362/14, de 6 de outubro de 2015, do TJUE, que opôs *Maximillian Schrems* contra *Data Protection Commisioner* (Comissão de Proteção de Dados Pessoais). [101]

Maximillian Schrems, utilizava a rede social *Facebook,* e derivado da situação levantada por *Edward Snowden*, quanto aos serviços da *National Security Agency*, o autor decidiu entender que, os Estados Unidos da América (EUA) não asseguravam um nível de segurança adequado de proteção dos dados pessoais transferidos, ao abrigo do «Porto Seguro». [102]

A decisão do acórdão, levou a que a CE, elaborasse um comunicado, que estabelece alternativas, para as transferências de dados pessoais para os EUA. [103]

---

[99] Considerando (101) e (102) do RGPD.

[100] Considerando (103) e (104) do RGPD.

[101] TJUE. (2015). Acórdão n.º C-362/14, de 06 de outubro de 2015. Acedido em 23 de maio de 2018. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=PT.

TJUE. (2015). Comunicado de Imprensa n.º 117/15, de 06 de outubro de 2015. Acedido em 23 de maio de 2018. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pt.pdf.

[102] The Courage Foundation. (2018). *In Support of Edward Snowden.* Acedido em 24 de maio de 2018. Disponível em https://edwardsnowden.com/.

[103] CE. (2015). COM (2015) 566 final. *Comunicação da Comissão ao Parlamento Europeu e do Conselho sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na*

Com o RGPD, as regras relativas às transferências de dados pessoais para um país terceiro são reforçadas. [104]

Contudo, quando não houver um nível de proteção adequado, os responsáveis pelo tratamento e subcontrates, só podem transferir dados pessoais para um país terceiro ou organização internacional, desde que sejam apresentadas garantias que assegurem os direitos dos titulares de dados.

As medidas adequadas, sem ser necessário uma autorização específica da ACI, vem elencadas no art.º 46.º, n.º 2 do RGPD, nomeadamente podem ser utilizadas para prever as garantias adequadas, sem requerer nenhuma autorização específica de uma autoridade de controlo. [105]

2. Sistema de balcão único (*One-Stop Shop)*

No âmbito da transferência de dados pessoais entre países terceiros ou organizações internacionais, o RGPD permite e incentiva à criação de um mecanismo, que permita um controlo mais efetivo e eficaz no tratamento de dados pessoais.

A criação do sistema de balcão único (*One-Stop-Shop*), ou seja, a ideia é obter uma ampla gama de serviços propostos num único gabinete, em que a transferência de dados em organizações multinacionais e o alargamento no âmbito de aplicação às entidades responsáveis pelo tratamento ou subcontratante de dados pessoais não localizadas na UE, ou para países terceiros, a autoridade de proteção de dados da sede da organização passa a assumir o controlo e supervisão de todos os outros estabelecimentos.

É um mecanismo, em que os responsáveis pelo tratamento e subcontratantes terão apenas de comunicar, com a autoridade de controlo principal, onde estiver o estabelecimento principal da organização, sendo que tal, afeta todos os outros estabelecimentos. [106]

---

*sequência do acórdão proferido pelo Tribunal de Justiça no processo C-362/14 (Schrem*s). Acedido em 25 de maio de 2018. Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0566&from=PT.

[104] CE. (2018). *Que regras se aplicam se a minha organização transferir dados para fora da UE?* Acedido em 21 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt.

[105] Considerando (108) e (109) do RGPD.

[106] Considerando (127) e (128) do RGPD.

3. As regras vinculativas aplicáveis às organizações

Conforme enuncia o art.º 4.º, n.º 20 do RGPD, entende-se por regras vinculativas aplicáveis (*Binding Corporate Rules*) às organizações e empresas, "*as regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta*."

Essencialmente, as regras aplicáveis às organizações, visam o tratamento dos dados pessoais, no processo de transferência de dados, para que sejam cumpridas, tanto pelo responsável e subcontratante numa organização sediada em Estado-Membro, como também fora da UE, ou seja, também abrange o responsável ou subcontratante de país terceiro. As regras vinculativas às empresas, estão consagradas no art.º 47.º do RGPD. [107]

[107] Art.º 47.º do RPGD: "*1. Pelo procedimento de controlo da coerência previsto no artigo 63.º, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, que devem: a) Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento; b) Conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e c) Preencher os requisitos estabelecidos no n.º 2. 2. As regras vinculativas aplicáveis às empresas a que se refere o n.º 1 especificam, pelo menos: a) A estrutura e os contactos do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta e de cada uma das entidades que o compõe; b) As transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão; c) O seu caráter juridicamente vinculativo, a nível interno e externo; d) A aplicação dos princípios gerais de proteção de dados, nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas; e) Os direitos dos titulares dos dados relativamente ao tratamento e regras de exercício desses direitos, incluindo o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado, nomeadamente a definição de perfis a que se refere o artigo 22.º, o direito de apresentar uma reclamação à autoridade de controlo competente e aos tribunais competentes dos Estados-Membros nos termos do artigo 79.º, bem como o de obter reparação e, se for caso disso, indemnização pela violação das regras vinculativas aplicáveis às empresas; f) A aceitação, por parte do responsável pelo tratamento ou subcontratante estabelecido no território de um Estado--Membro, da responsabilidade por toda e qualquer violação das regras vinculativas aplicáveis às empresas cometida por uma entidade envolvida que não se encontre estabelecida na União; o responsável pelo tratamento ou o subcontratante só pode ser exonerado dessa responsabilidade, no todo ou em parte, mediante prova de que o facto que causou o dano não é imputável à referida entidade; g) A forma como as informações sobre as regras vinculativas aplicáveis às empresas, nomeadamente, sobre as disposições referidas nas alíneas d), e) e f) do presente número, são comunicadas aos titulares dos dados para além das informações referidas nos artigos 13.o e 14.º; h) As funções de qualquer encarregado da proteção de dados, designado nos termos do artigo 37.º ou de qualquer outra pessoa ou entidade*

Ou seja, se for averiguado que um país terceiro, não assegura um tratamento com um nível de segurança adequado de proteção de dados, a transferência de dados deverá ser proibida. No entanto, tal poderá ser colmatado se, forem cumpridas as normas do RGPD, as regras vinculativas e derrogações para situações específicas. [108]

A aprovação das regras vinculativas às empresas, devem seguir vários procedimentos de aprovação, de modo a escolher a Autoridade de Controlo Principal (ACP). [109]

As regras aplicáveis às empresas, nas organizações multinacionais, que nomeadamente tenham um sítio na internet, por exemplo, divulgam as suas regras para dar conhecimento ao titular de dados pessoais, no que acontece em caso de transferência de dados. [110]

Para facilitar e, poder controlar o processo de transferência de dados pessoais numa organização multinacional, que transfira dados pessoais para um responsável ou subcontratante num país terceiro, o sistema de balcão único, é um mecanismo que possibilita a ACP, acompanhar todos os procedimentos que afetem tanto a organização principal como todos os outros estabelecimentos conexos, de modo a consolidar o nível de segurança adequado no tratamento de dados pessoais.

---

responsável pelo controlo do cumprimento das regras vinculativas aplicáveis às empresas, a nível do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, e pela supervisão das ações de formação e do tratamento de reclamações; i) Os procedimentos de reclamação; j) Os procedimentos existentes no grupo empresarial ou no grupo de empresas envolvidas numa atividade económica conjunta para assegurar a verificação do cumprimento das regras vinculativas aplicáveis às empresas. Esses procedimentos incluem a realização de auditorias sobre a proteção de dados e o recurso a métodos que garantam a adoção de medidas corretivas capazes de preservar os direitos dos respetivos titulares. Os resultados dessa verificação devem ser comunicados à pessoa ou entidade referida na alínea h) e ao Conselho de Administração da empresa ou grupo empresarial que exerce o controlo ou do grupo de empresas envolvidas numa atividade económica conjunta, devendo também ser facultados à autoridade de controlo competente, a pedido desta; k) Os procedimentos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controlo; l) O procedimento de cooperação com a autoridade de controlo para assegurar o cumprimento, por qualquer entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, em especial facultando à autoridade de controlo os resultados de verificações das medidas referidas na alínea j); m) Os procedimentos de comunicação, à autoridade de controlo competente, de todos os requisitos legais a que uma entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas; e n) Ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal."

[108] Considerando (107) , (108) e (110) do RGPD.

[109] CE. (2018). *Corporate rules for data transfers within multinational companies.* Acedido em 26 de maio de 2018. Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corpora te-rules_en.

[110] Hewlett-Packard Company. (2018). *O que são as regras vinculativas das empresas (BCR - Binding Corporate Rules) da HP*. Acedido em 26 de maio de 2018. Disponível em http://www8.hp.com/pt/pt/binding-corporate-rules.html.

CAPÍTULO VII – AUTORIDADE DE CONTROLO INDEPENDENTE

1. O fim das notificações e autorizações

Entende-se por ACI, "*uma autoridade pública independente criada por um Estado-Membro*," *vide* art.º 4.º, n.º 20 do RGPD. Os termos em que a mesma exerce os seus poderes, estão previstos no art.º 51.º do RGPD, "*a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União*." No ordenamento jurídico português a ACI competente em matéria de proteção de dados, é a CNPD.

Novamente, e focando o tema da implementação do RGPD, há uma alteração de paradigma quanto às notificações e autorizações, principal fonte de rendimento da CNPD, que agora passa a ter um perfil de entidade fiscalizadora.

As ACI dos Estados-Membros, assumem um papel importante na fiscalização e cumprimento do regulamento nas organizações. Durante a aplicação da D95, as organizações tinham a obrigação de notificar a ACI, para que fosse autorizado o tratamento de dados pessoais.

Com o desaparecimento da obrigação de notificar, e consequente autorização, a ACI, torna-se como foi referido, um órgão fiscalizador no cumprimento do RGPD. Ou seja, há uma mudança de paradigma. Os responsáveis pelo tratamento de dados e subcontratantes, tem de demonstrar capacidade, de a todo o momento, serem capazes de assegurar um nível de proteção adequado dos dados pessoais. Ou seja, o foco da ACI passa para as organizações, obrigando estas a cumprir as normas do regulamento. [111]

2. Estatuto, competência, atribuições e poderes

As ACI, agem com "*total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do regulamento*," *vide* art.º 52.º, n.º 1 do RGPD.

Ou seja, as ACI são dotadas de autonomia no exercício das suas funções, que especificamente, são da matéria de proteção de dados pessoais. Os membros das ACI, "*devem*

[111] Considerando (122) e (123) do RGPD.

possuir habilitações, experiência e conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados," *vide* art.º 53.º, n.º 2 do RGPD.

A constituição da ACI está dependente dos pressupostos do art.º 54.º do RGPD e quanto às atribuições de poderes, segundo o art.º 57.º do mesmo regulamento.

Tal, já se observava na D95 nas competências atribuídas, contudo, há um aumento de regras no capítulo do RGPD correspondente às ACI, nomeadamente na criação do conceito de ACP, por força, do tratamento transfronteiriço de dados pessoais, *vide* art.º 56.º, n.º 1 do RGPD.

Ou seja, passará a haver uma total cooperação das ACI dos Estados-Membros, no tratamento de dados pessoais, em especial, no caso de transferência de dados pessoais.

3. Cooperação entre as autoridades de controlo independentes e assistência mútua

A necessidade de cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas, surge essencialmente, com o intuito de alcançar um consenso, nas informações trocadas entre si.

A título de exemplo, surge o Acórdão n.º C-230/14, de 01 de outubro de 2015, do TJUE, que opôs a *Weltimmo* contra *Nemzeti Adatvédelmi és Információszabadság Hatóság* (ANHPD – Autoridade Nacional Húngara para a Proteção de Dados e Liberdade de Informação). [112]

No caso em questão, a *Weltimmo* "*uma sociedade registada na Eslováquia, gere um sítio da internet de anúncios de imóveis situados na Hungria. Neste âmbito, procede ao tratamento de dados pessoais dos anunciantes. Os anúncios são publicados de forma gratuita durante um mês, passando a ser pagos após este período. Um elevado número de anunciantes solicitou, por correio eletrónico, a retirada dos respetivos anúncios no fim do primeiro mês e, na mesma ocasião, o apagamento dos seus dados pessoais. No entanto, a Weltimmo não procedeu a esse apagamento e faturou o preço dos seus serviços aos interessados. Por os montantes faturados não terem sido pagos, a Weltimmo comunicou os dados pessoais dos anunciantes a empresas de recuperação de crédito*." [113]

[112] TJUE. (2015). Acórdão n.º C-230/14, de 01 de outubro de 2015. Acedido em 26 de maio de 2018. Disponível em http://curia.europa.eu/juris/document/document.jsf?docid=168944&mode=req&pageIndex=1&dir=&occ=first& part=1&text=&doclang=PT&cid=541244.

[113] TJUE. (2015). Comunicado de Imprensa n.º 111/15, de 01 de outubro de 2015. Acedido em 26 de maio de 2018. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150111pt.pdf.

A referida sociedade, pretendeu impugnar a decisão contra a ANHPD, por referir que a autoridade húngara não teria competência para aplicar a coima prevista na lei. Contudo, no Acórdão em análise, o TJUE, para determinar o direito aplicável pela autoridade de controlo competente do respetivo Estado-Membro, deve corresponder àquela competência territorial em que a organização mantém o seu estabelecimento principal,

Assim o TJUE, responde à questão da autoridade de controlo, quanto à competência para aplicar sanções: "*a aplicação territorial dos poderes de cada autoridade de controlo é confirmada pelo artigo 28.º, n.º 6 desta diretiva, que enuncia que cada autoridade de controlo é competente para exercer no território do seu Estado-Membro os poderes que lhe foram atribuídos em conformidade com o artigo 28.º, n.º 3, da referida diretiva, independentemente do direito nacional aplicável. Este artigo 28.º, n.º 6, precisa também que cada autoridade pode ser solicitada a exercer os seus poderes por uma autoridade de outro Estado-Membro e que as autoridades de controlo cooperarão entre si na medida do necessário ao desempenho das suas funções, em especial através do intercâmbio de quaisquer informações úteis*." [114]

Neste sentido, o RGPD, alterou o paradigma quanto à cooperação entre autoridades de controlo. O GT29, elaborou um conjunto de orientações nesta temática. [115]

O princípio do balcão único, não é tão somente um mecanismo de comunicação entre a ACP e o tratamento de dados transfronteiriços das organizações com outros responsáveis e subcontratantes de países terceiros, também permite que as várias ACI, em conjunto com a ACP, possam assistir-se mutuamente, *vide* art.º 61.º do RGPD, e conduzir operações conjuntas, *vide* art.º 62.º do RGPD, com vista a colmatar lacunas, em casos de tratamento de dados pelo responsável e o subcontratante, em que seja necessário investigar, inspecionar e tomar medidas de execução para assegurar o cumprimento do RGPD de forma mais coerente. [116]

Conforme se observa, pela implementação do regulamento em contraste com a D95, há uma alteração de paradigma no auxílio entre ACI. De forma a assegurar, o "*cumprimento do RGPD de forma mais coerente,*" passa a haver um intercâmbio de informações úteis entre si.

[114] TJUE. (2015). Acórdão n.º C-230/14. Cit. 98. Parágrafo 52.
[115] GT29. (2016). *Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante*. WP 244 ver.01. Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.
[116] Considerando (133), (134), (135) e (136) do RGPD.

CAPÍTULO VIII – VIAS DE RECURSO E SANÇÕES

1. Direitos dos titulares no âmbito da proteção dos dados

Os titulares de dados pessoais, além dos direitos apresentados quanto ao tratamento de dados pessoais, quando esses direitos são violados, podem os mesmos recorrer a ações judiciais que possam efetivar a defesa dos seus direitos e liberdades.

Falamos nomeadamente nas vias de recurso, responsabilidade e sanções, segundo os artigos 77.º e seguintes do RGPD.

O direito de apresentar reclamação a uma ACI, *vide* art.º 77.º, n.º 1 do RGPD, permite ao titular de dados pessoais "*o direito a apresentar reclamação a uma autoridade de controlo.*" Ou seja, o titular de dados pessoais, pode recorrer a uma autoridade competente na matéria de dados pessoais. [117]

O direito à ação judicial contra uma ACI, *vide* art.º 78.º do RGPD. Este direito assiste o titular de dados pessoais, caso a reclamação não seja tratada ou não seja informado do andamento ou resultado da reclamação. Nesta situação, a ACI poderá responder judicialmente, caso não se verifique os pressupostos quanto ao pedido de reclamação do titular de dados pessoais.

O direito à ação judicial contra um responsável pelo tratamento ou um subcontratante. Nesta matéria, como já foi referido anteriormente, é atribuída responsabilidade pelo tratamento de dados pessoais. Esta responsabilidade é extensível a quem trata, sendo o responsável, como também ao subcontratante. Neste sentido, o titular de dados pessoais pode recorrer do art.º 79.º do RGPD, de modo, a requerer ação judicial, caso os responsáveis pelo tratamento de dados, violem os direitos que assistem ao titular, na sequência do tratamento de dados.

Na representação do titular de dados pessoais, pode o mesmo, ter direito de mandatar um "*organismo, organização ou associação sem fins lucrativos*," em que a sua "*atividade abranja a defesa dos direitos e liberdades do titular de dados pessoais,*" para que em seu nome, apresente reclamação, *vide* art.º 80.º, n.º 1 do RGPD. Ou seja, o titular de dados pessoais, não tem que necessariamente agir por conta própria. É-lhe facultada a possibilidade de ser acompanhado no processo de reclamação, segundo o RGPD. [118]

[117] Considerando (141) do RGPD.
[118] Considerando (142) do RGPD.

Se de facto, observar-se que o titular de dados pessoais sofre danos materiais ou imateriais devido a uma violação segundo o RGPD, o titular tem o direito de receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Neste sentido, o titular tem direito de indeminização pela responsabilidade no tratamento de dados pessoais, segundo o art.º 82.º do RGPD. [119]

Ou seja, para além dos direitos consagrados no RGPD, que protegem o titular de dados pessoais nos seus direitos e liberdades, também o mesmo em caso de violação desses mesmos direitos, pode recorrer à via judicial, junto das autoridades competentes na matéria de dados pessoais.

Há de facto, uma alteração de paradigma no que concerne aos direitos do titular de dados pessoais. O reforço das leis e o alargamento de competências da ACI, levam a que haja uma nova consciencialização, diria mais, um reforço da sensibilização, no tratamento de dados pessoais, às organizações.

2. Aplicação de coimas e sanções: condições gerais

O maior receio das organizações com a implementação do RGPD. O referido regulamento nos artigos 83.º e 84.º do RGPD, prevê a aplicação de coimas e consequentes sanções em caso de incumprimento das normas do regulamento. [120]

As coimas pelo incumprimento do RGPD, entram em vigor a partir de 25 de maio de 2018, pelo que no caso português, a Proposta de Lei n.º 120/XIII ainda está em debate e já levantou algumas opiniões controversas acerca das organizações isentas, nomeadamente as organizações públicas. [121]

As coimas, segundo o regulamento podem atingir no máximo 4% do volume anual de negócios ou 20 000 000 de euros, *vide* art.º 83.º, n. º 5 do RGPD.

Em Portugal, na referida Proposta de Lei, o incumprimento das normas relativamente ao tratamento de dados pessoais, abrangem não só as organizações de grandes dimensões, mas também as pequenas e médias empresas, e as pessoas singulares. As coimas previstas consoante os casos: de 2 500 a 10 000 000 de euros ou 2% do volume de negócios anual, a nível mundial,

[119] Considerando (146) do RGPD.
[120] Considerando (148) do RGPD.
[121] SapoTek. (2018). *RGPD: Presidente da CNPD considera "chocante" que Governo possa isentar organizações públicas de coimas.* Acedido em 27 de maio de 2018. Disponível em https://tek.sapo.pt/noticias/negocios/artigos/rgpd-presidente-da-cnpd-considera-chocante-que-governo-possa-isentar-organizacoes-publicas-de-coimas.

conforme o que for mais elevado, tratando-se de grande empresa; de 1 000 a 1 000 000 euros ou 2% do volume de negócios anual, a nível mundial, conforme o que for mais elevado, tratando-se de pequena ou média empresa; de 500 a 250 000 euros, no caso de pessoas singulares. [122]

Contudo, o RGPD prevê que seja atribuído um EPD, conforme já foi mencionado anteriormente, consoante o tipo de tratamento de dados pessoais, mas que não invalida a contratação do mesmo em regime de prestação de serviços, tanto para organizações do setor privado, mas também para o setor público.

A respeito da aplicação de coimas, o GT29 elaborou um conjunto de orientações nesta temática. [123]

Os princípios a ter em conta na aplicação de coimas devem: "*respeitar o conceito de equivalência; ser efetivas, proporcionadas e dissuasivas; aplicáveis a cada caso em concreto; promover a cooperação entre as várias ACI.*" [124]

[122] Considerando (149) do RGPD.

[123] GT29. (2016). Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679. WP 253. Acedido em 23 de maio de 2018. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[124] *ibid*. GT29. (2016). Cit. 123. pp. 5-8.

CONCLUSÃO

A decisão de mudar o paradigma na proteção de dados pessoais, é certamente, algo que veio tornar as organizações mais conscientes para esta temática. Neste sentido, a CE, de modo a analisar o impacto das novas tecnologias na vida dos cidadãos europeus, procedeu à recolha de dados sobre o conhecimento acerca desse impacto. O relatório permitiu averiguar que "*não houve surpresa de que os cidadãos europeus utilizam os serviços digitais diariamente, ..., que, não tem controlo sobre o tratamento de dados pessoais, e que estão preocupados com a falta de controlo.*" [125]

O debate sobre a implementação do RGPD em Portugal, iniciou-se, em conferência na Assembleia da República. [126]

No entanto, o regulamento está aí, e o debate continua, com a Proposta de Lei n.º 120/XIII, que procederia à revogação da Lei n.º 67/98, de 26 de outubro.

Neste momento, havendo necessidade de o titular de dados pessoais recorrer aos seus direitos, por força da regulamentação da União Europeia, os Estados-Membros estão sujeitos às suas normas, ou seja, aplica-se o RGPD, que fora aprovado em 2016, para defesa dos direitos e liberdades das pessoais singulares no tratamento de dados pessoais.

A análise ao RGPD, permitiu constatar, uma alteração de paradigma. Um novo conceito. Um reforço do que já se conhecia, mas que agora, é definitivamente do conhecimento de qualquer cidadão da UE, de que o direito à proteção de dados pessoais se acaba de tornar uma consciencialização de que o tratamento, tanto pelas organizações como pelos titulares dos dados pessoais, está sujeito a responsabilidades e consequentes coimas.

No conjunto de direitos do titular de dados pessoais, evidenciam-se, o direito ao consentimento e o direito a ser esquecido. As organizações devem fornecer informações ao titular de dados pessoais acerca, das finalidades da recolha de dados pessoais. Sendo que essas informações devem abranger, se o tratamento assegura um nível adequado de proteção dos dados pessoais pelo responsável e subcontratante. Essas informações devem ser transparentes.

---

[125] CE (2015). *Special Eurobarometer 431: Data Protection*. Acedido em 27 de maio de 2018. Disponível em http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2075.

[126] Assembleia da República TV. (2016). O Novo Regulamento Europeu de Proteção de Dados – Que desafios? Que oportunidades? – Sessão da Manhã: http://www.canal.parlamento.pt/?cid=1296&title=conferencia-comissao-nacional-de-protecao-de-dados-manha

Assembleia da República TV. (2016). O Novo Regulamento Europeu de Proteção de Dados – Que desafios? Que oportunidades? – Sessão da Tarde: http://www.canal.parlamento.pt/?cid=1297&title=conferencia-comissao-nacional-de-protecao-de-dados-tarde

As organizações devem informar os titulares de dados pessoais de forma inteligível, fácil acesso, objetiva e utilizando um linguagem clara e de simples compreensão.

Por implementação do RGPD, o leque de definição de dados pessoais em contraste com a D95 aumentou, passando a abranger os dados biométricos e de saúde.

O fim das notificações e autorizações por parte da ACI, em que esta passa a afigurar como uma entidade fiscalizadora, pelo que agora o foco do cumprimento do RGPD passa a ser um papel fundamental nas organizações.

O surgimento de uma nova profissão, o Encarregado de Proteção de Dados (EPD) que passará a afigurar nos quadros da organização, de forma a que as suas funções não surtam conflito de interesses. A nomeação de um EPD, visa essencialmente assegurar que a organização cumpre o regulamento.

No processamento de dados do titular de dados pessoais, as organizações devem antecipadamente averiguar o impacto na proteção de dados, e adotar medidas de segurança que impossibilitem a violação dos mesmos, de forma a aliviar esses riscos.

Por fim, o RGPD prevê a aplicação de coimas que podem ir até 4% do volume de negócios global anual ou 20 milhões de euros. Sendo que no ordenamento jurídico português, por força da aplicação do regulamento, a lei referente à proteção de dados, que ainda se encontra em debate, deverá implementar sanções especificamente aplicáveis às pequenas e médias empresas, e pessoas singulares.

REFERÊNCIAS BIBLIOGRÁFICAS

Obras Impressas

LAMBERT, Paul. (2017). ***The Data Protection Officer***. First Edition. Taylor & Francis Group

Artigos Eletrónicos

Agencia Española de Protección de Datos. (2018). ***Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD***. Disponível em https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

AUSLOOS, Jef. (2012). ***The right to be forgotten – Worth remembering?*** Computer Law & Security Review. Volume 28. Issue 2. pp. 143-152. Elsevier Ltd. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364912000246?via%3Dih_ub. doi: 10.1016/j.clsr.2012.01.006

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. (2017). ***The Standard Data Protection Model***. Disponível em https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2017/04/SDM-Methodology_V1_EN1.pdf

Comissão Europeia. (2010). COM (2010) 609 final. ***Uma abordagem global da proteção de dados pessoais na União Europeia.*** Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2010:0609:FIN

Comissão Europeia. (2012). COM (2012) 11 final. ***Proposta de regulamento relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.*** Disponível em https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2012:0011:FIN

Comissão Europeia. (2015). COM (2015) 566 final. ***Comunicação da Comissão ao Parlamento Europeu e do Conselho sobre a transferência de dados pessoais da UE para os Estados Unidos da América ao abrigo da Diretiva 95/46/CE na sequência do acórdão***

proferido pelo Tribunal de Justiça no processo C-362/14 (Schrems). Disponível em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0566&from=PT

Comissão Europeia. (2015). ***Special Eurobarometer 431: Data Protection.*** Disponível em http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_sum_en.pdf

Comissão Europeia. (2018). ***Como posso aceder aos meus dados pessoais detidos por uma empresa/organização?*** Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/how-can-i-access-my-personal-data-held-company-organisation_pt

Comissão Europeia. (2018). ***O que significa a proteção de dados «desde a conceção» e «por defeito»?*** Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt

Comissão Europeia. (2018). ***Posso pedir a uma empresa que apague os meus dados pessoais?*** Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-delete-my-personal-data_pt

Comissão Europeia. (2018). ***Posso pedir a uma empresa que cesse o tratamento dos meus dados?*** Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-ask-company-organisation-stop-processing-my-personal-data_pt

Comissão Europeia. (2018). ***Que regras se aplicam se a minha organização transferir dados para fora da UE?*** Disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pt

Comissão Nacional de Proteção de Dados. (2018). ***10 Medidas para preparar a aplicação do Regulamento Feral de Proteção de Dados.*** Disponível em https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf

Grupo de Trabalho do Artigo 29.º. (2016). ***Guidelines on consent under Regulation 2016/679***. WP 259 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Grupo de Trabalho do Artigo 29.º. (2016). ***Guidelines on transparency under Regulation 2016/679***. WP 260 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Grupo de Trabalho do Artigo 29.º. (2016). ***Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679***. WP 248 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Grupo de Trabalho do Artigo 29.º. (2016). ***Orientações sobre o direito à portabilidade dos dados***. WP 242 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Grupo de Trabalho do Artigo 29.º. (2016). ***Orientações sobre os encarregados da proteção de dados (EPD)***. WP 243 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Grupo de Trabalho do Artigo 29.º. (2016). ***Perguntas Frequentes***. Anexo WP 242 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Grupo de Trabalho do Artigo 29.º. (2017). ***Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679***. WP 251 rev.01. Disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Hewlett-Packard Company. (2018). ***O que são as regras vinculativas das empresas (BCR - Binding Corporate Rules) da HP***. Disponível em http://www8.hp.com/pt/pt/binding-corporate-rules.html

Information Commissioner's Office. (2018). Reino Unido. ***Código de Prática de Avaliações de Impacto de Privacidade***. Disponível em https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

International Organization for Standardization. ***ISO/IEC 29100:2011***. Disponível em https://www.iso.org/standard/45123.html

International Organization for Standardization. ***ISO/IEC 29134:2017***. Disponível em https://www.iso.org/standard/62289.html

International Organization for Standardization. ***ISO/IEC 27005:2011***. Disponível em https://www.iso.org/standard/56742.html

International Organization for Standardization. ***ISO/IEC 27005:2011***. Disponível em https://www.iso.org/standard/54534.html

The Guardian. (2017). ***Uber concealed massive hack that exposed data of 57m users and drivers***. Disponível em https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 70/14***. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070pt.pdf

Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 110/15***. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110pt.pdf

Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 111/15***. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150111pt.pdf

Tribunal de Justiça da União Europeia. (2015). ***Comunicado de Imprensa n.º 117/15***. Disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pt.pdf

Acórdãos

Tribunal de Justiça da União Europeia – Acórdão de 13 de maio de 2014, Processo n.º C-131/12 (***Google Spain***)

Tribunal de Justiça da União Europeia – Acórdão de 1 de outubro de 2015, Processo n.º C-201/14 (***Smaranda Bara***)

Tribunal de Justiça da União Europeia – Acórdão de 1 de outubro de 2015, Processo n.º C-230/14 (***Weltimmo***)

Tribunal de Justiça da União Europeia – Acórdão de 6 de outubro de 2015, Processo n.º C-362/14 (***Schremms***)

Páginas Eletrónicas

Assembleia da República (Proposta de Lei n.º 120/XIII): https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

Assembleia da República TV. (2016). ***O Novo Regulamento Europeu de Proteção de Dados – Que desafios? Que oportunidades? – Sessão da Manhã****:* http://www.canal.parlamento.pt/?cid=1296&title=conferencia-comissao-nacional-de-protecao-de-dados-manha

Assembleia da República TV. (2016). ***O Novo Regulamento Europeu de Proteção de Dados – Que desafios? Que oportunidades? – Sessão da Tarde***: http://www.canal.parlamento.pt/?cid=1297&title=conferencia-comissao-nacional-de-protecao-de-dados-tarde

Base de Dados da União Europeia: http://eur-lex.europa.eu/homepage.html

Comissão Europeia (Proteção de Dados):
https://ec.europa.eu/info/law/law-topic/data-protection_pt

Comissão Europeia (Mercado Único Digital):
https://ec.europa.eu/commission/priorities/digital-single-market_pt#policy-areas

Comissão Nacional de Proteção de Dados:
https://www.cnpd.pt/

Grupo de Trabalho do Artigo 29.º:
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

ISO:
https://www.iso.org/standards.html

SapoTek:
https://tek.sapo.pt/

Sage:
https://www.sage.pt/

The Courage Foundation:
https://edwardsnowden.com/

The Guardian:
www.theguardian.com/

União Europeia:
https://europa.eu/european-union/index_pt