UNIVERSIDADE CATÓLICA PORTUGUESA

Faculdade de Direito do Porto

Mestrado em Direito Geral

Tese de Mestrado

O E-Commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados – A Uniformização na União Europeia

Marta Laís dos Santos Alegria Couto

Orientador: Professor Manuel Oehen Mendes

Porto
Outubro, 2016

Aos meus pais,

À minha família,

Aos meus amigos.

"O êxito da vida não se mede pelo caminho que conquistamos, mas sim pelas dificuldades que superamos ao longo do caminho."

Abraham Lincoln

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer ao Professor Manuel Oehen Mendes por ter aceite ser o orientador da minha tese. Desde já agradeço toda a sua ajuda e disponibilidade no que diz respeito à partilha do seu conhecimento, às dicas que me foi transmitindo a longo das nossas reuniões, à sugestão de diversas referências bibliográficas que tiveram todo o interesse para o desenvolvimento deste trabalho e todo o apoio prestado ao longo do caminho percorrido até à conclusão da minha tese.

Presto, também, todos os agradecimentos aos meus familiares e amigos por me apoiarem em todo este percurso e por terem contribuído de alguma forma para que tudo fosse possível de concretizar.

Dedico, assim, a minha maior gratidão a todos os que estiveram presentes nesta importante etapa da minha vida.

RESUMO

A presente dissertação terá como principal objectivo desenvolver o tema sobre o E – Commerce visto na prespectiva do Direito.

Assim, debruçando-me na atualidade decidi, em consonância com opinião do meu orientador, Prof. Manuel Oehen Mendes, especificar este tão vasto tema e, uma vez que, recentemente surgiu o novo Regulamento Geral da Proteção de Dados da União Europeia, consideramos que seria interessante analisar o mesmo, e tirar daí algumas conclusões.

Como analisaremos mais adiante, cada Estado – Membro da União Europeia já havia elaborado algumas leis e diretivas a fim de regular as questões relativas ao E – commerce mas, de forma a criar uma uniformização de regras no âmbito da União Europeia, foi, então, elaborado um único regulamento com o intuito de regular esta matéria num contexto global.

Desta forma, optamos, então, por cingir o tema desta dissertação para a questão da proteção de dados, sendo que, como tem havido um aumento bastante significativo no que concerne à utilização do E – commerce, surgiu a necessidade de assegurar que todos os dados que são colocados à disposição de "instituições online" são protegidos e que a informação pessoal de cada utilizador está, de facto, em segurança.

Palavras – Chave: E – Commerce; Direito; Proteção de Dados; Regulamento Geral da Proteção de Dados da União Europeia.

ABSTRACT

This work will primarily aim to develop the theme of the E - Commerce seen in the perspective of law.

Thus, leaning in our days i decided, in accordance with the opinion of my advisor, Prof. Manuel Oehen Mendes, specify this vast subject and, since recently emerged the new General Regulation of the European Union Data Protection, we believe it would be interesting to analyze it and draw some conclusions.

As discussed later, each Member - State of the European Union had already drafted some laws and directives to regulate matters relating to e - commerce but in order to create uniform rules within the European Union, was then prepared a single Regulation to handle with this matter in a global context.

Thus, we decided then to gird the subject of this thesis to the issue of data protection, and, as there has been a very significant increase in relation to the use of E - commerce, the need to ensure that all data which are made available to "online institutions" are protected and that the personal information of each user is in fact safe.

Key – Words: E – Commerce; Right; Data Protection; General Rules of Data Protection of European Union.

LISTA DE ABREVIATURAS

CDF – Carta dos Direitos Fundamentais

CE – Comissão Europeia

CNPD – Comissão Nacional da Proteção de Dados

CRP – Constituição da República Portuguesa

LPDP – Lei da Proteção de Dados Pessoais

RGPD – Regulamento Geral da Proteção de Dados da União Europeia

UE – União Europeia

PREFÁCIO

A escolha do tema da minha dissertação foi motivada, essencialmente, pelo gosto pessoal.

Aprecio, de facto, esta nova vertente de ser possível comprar produtos via on-line, sou utilizadora deste novo conceito e considero que seria um tema bastante interessante, na medida em que, tenho todo o interesse de perceber como é que o E – Commerce funciona à luz da aplicabilidade legal.

Uma vez que criei, à relativamente pouco tempo, uma marca de blusas de senhora para competição no âmbito de uma modalidade desportiva, a Equitação, seria para mim, de todo importante entender todas as questões que estão inerentes a este tema, tendo em vista uma possível criação de comercialização online das mesmas.

Assim, o desenvolvimento deste trabalho permitiu-me adquirir um conhecimento mais aprofundado do tema e, compreender como está regulada esta matéria, tendo em conta a sua aplicação prática.

Uma vez que se trata de um tema profundamente atual, sendo o mesmo discutido recentemente a nível Europeu, não poderia deixar de considerar o tema tremendamente adequado, face à atualidade.

Todo este trabalho se foi desenvolvendo de uma forma harmoniosa, com toda a colaboração necessária para a elaboração do mesmo.

Todo este trabalho foi desenvolvido com muito gosto e empenho.

As expectativas foram alcançadas.

INTRODUÇÃO

O tema da minha dissertação é "O E – Commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados – A Uniformização na União Europeia".

Para a elaboração deste trabalho, debruçei-me fundamentalmente no Regulamento Geral da Proteção de Dados da União Europeia, sendo este aprovado recentemente, após longos períodos de discussão, que trata a matéria dos dados pessoais e sua proteção.

Este trabalho, é então composto por vários títulos e subtítulos e o seu principal objectivo é abordar as matérias que tiveram mais ênfase e que se "estrearam" no novo Regulamento da Proteção de Dados da União Europeia.

Assim, primeiramente enquadrei o tema do E – Commerce com o próprio Regulamento e de seguida faço uma abordagem histórica do mesmo, referindo as leis que já existiam e como é que foi possível chegar à publicação definitiva deste Regulamento, fazendo também uma breve menção das novas matérias constituintes deste diploma.

De seguida, como forma de dar uma introdução simples ao tema, começo por esclarecer alguns conceitos essenciais que lhe estão inerentes, como o conceito de dados pessoais, de tratamento de dados e do conceito de consentimento.

Posteriormente, começo então por referir e definir três novos direitos, que constam agora do Regulamento: o Direito da Portabilidade dos Dados; o Direito ao Esquecimento; e o Direito de Oposição ao Tratamento de Dados.

Faço, depois, uma abordagem relativamente aprofundada no que diz respeito às questões dos princípios e legalidade, decorrentes do tratamento dos dados pessoais que são recolhidos, fazendo referência a algumas questões importantes como: a finalidade do tratamento de dados, a base jurídica do mesmo e a questão do interesse legitimo.

De seguida procedo a uma análise da matéria de obrigação dos responsáveis de dados/ subcontratantes, matéria essa que também teve algum ênfase neste Regulamento, abordando os parâmetros mais pertinentes.

De seguida, debrucei – me na matéria que diz respeito ao regime de fiscalizações e sanções e, por fim, tratei das questões relativas à proteção de dados especial (como por exemplo, o caso de dados sensíveis), referindo ainda um caso que apareceu recentemente em reportagens televisivas.

Para concluir, elaborei um pequeno texto/comentário face àquelas que serão consideradas prespectivas para o futuro, terminando assim este trabalho com uma vertente futurista.

ÍNDICE

1. ENQUADRAMENTO

1.1. O E – Commerce e o Regulamento Geral da Proteção de Dados

Nos últimos anos houve uma evolução significativa no que concerne à tecnologia. Tal permitiu que o mundo interagisse em maior velocidade e os mercados alcançassem uma grande dinamização.

De facto, a evolução que se foi sentindo permitiu que olhássemos para o Mundo de outra forma. Na verdade, a internet veio dar-nos uma visão de um Mundo mais pequeno, em que tudo é possível com apenas um click. Hoje, qualquer pessoa pode chegar rapidamente ao outro canto do Mundo, acedendo facilmente a serviços e produtos que outrora estariam a longos quilómetros de distância. E, é desta forma que surge o E-Commerce – definido como qualquer tipo de negócio ou transação comercial que implica a transferência de informação através da internet". Este, traduz – se na realização de diversos tipos de negócios, entre os quais, o comércio de bens e serviços através de sites à disposição do utilizador.

Na verdade, o E – Commerce é, atualmente, um dos grandes fenómenos da Internet, sendo certo que o seu recurso está em larga expansão. No entanto, se recuarmos um pouco no tempo, percebemos que este crescimento tem sido gradual, sendo que, na década de 1990 o E – Commerce mostrava-se como um fenómeno tipicamente norte – americano, uma vez que as instituições online que tinham maior afluência eram a Amazon.com e o E-bay, instituições essas que não eram, à partida, acessíveis para todas as economias mundiais, uma vez que nem todos os países tinham uma boa acessibilidade à informação. Desta forma, foi necessária uma adaptação gradual a todo este contexto de mudança, sendo este o principal obstáculo à proliferação do E – Commerce, em que cada país teve de adaptar-se ao seu próprio ritmo. Apesar de o E – Commerce ser, ainda, um conceito de alguma forma recente, uma vez que, embora tenha dado os seus primeiros passos na década de 1990 só se tornou num conceito consistente no início do século XXI, tem sido notório o esforço de adaptação e confiança impostos no mesmo pelos seus utilizadores. Assim, a globalização deste novo conceito permitiu que as pequenas e médias empresas conseguissem beneficiar de uma estratégia comercial num contexto internacional,

direcionada para a venda online. Desta forma, podemos dizer que o E – commerce está a transformar-se em algo "viral", sendo interpretado como uma tecnologia de informação e comunicação que tem como foco a sua evolução mundial.

Duas das grandes exigências do "hoje" é a rapidez e qualidade. Tal só foi possível alcançar com o desenvolvimento tecnológico, que permitiu criar o comércio electrónico, onde nos é possível aceder a tudo o que desejamos em qualquer lugar, a qualquer hora.

Existem notórias vantagens no que toca à utilização do E – Commerce, na medida em que hoje existe um diversificado leque de opções de escolha e de oferta; por conseguinte os preços podem ser ajustados à necessidade de cada um, uma vez que há mais competitividade e, por isso, não existem muitas disparidades de preço; hoje em dia é fácil aceder a qualquer produto ou serviço mesmo estando fisicamente longe; por sua vez existe uma maior capacidade de resposta dada a fácil acessibilidade e, podemos constatar que tudo isto permitiu que houvesse um aumento significativo no que toca à utilização do comércio on-line.

No entanto, face a esta evolução, surgiram algumas questões de extrema importância, sendo que a utilização do comércio electrónico traz também algumas preocupações aos seus utilizadores, como por exemplo: como se pode assegurar aos utilizadores que os dados que os mesmos colocam à disposição de cada "instituição on-line" é protegida? Este foi o principal motivo que deu origem à necessidade de legislar esta matéria.

Assim, para regular a questão da proteção de dados, e depois de várias Diretivas existentes, surge então o "Regulamento Geral da Proteção de Dados da UE" que, para além de estabelecer determinados parâmetros de forma a garantir essa segurança, cria uma lei geral, uniformizando a Lei da União Europeia. Uma vez que o direito à proteção constituí um direito fundamental do Homem, consagrado na Constituição, este Regulamento, não só é importante a nível europeu mas reforça ainda a proteção nacional de cada Estado – Membro da União Europeia. Ainda, o Parlamento Europeu sempre mostrou a intenção de encontrar um equilíbrio no que concerne à melhoria da segurança e proteção versus preservação dos direitos do cidadão e à preservação da sua privacidade.

Desta forma, a reforma da proteção de dados da União Europeia vem dar ênfase a esses direitos, possibilitando a que os cidadãos alcancem um maior controlo face aos seus dados e garantam a sua proteção.

1.2. Breve Abordagem Histórica do Regulamento Geral da Proteção de Dados

Com a preocupação de acompanhar o desenvolvimento tecnológico e a proliferação do comércio electrónico que se foi sentindo ao longo dos tempos, houve a necessidade de estabelecer determinadas regras de forma a regular as questões que lhes estão inerentes. Assim, no que diz respeito ao nosso ordenamento jurídico foram várias as leis que surgiram nesse sentido, como:

a) Em primeiro lugar, a Constituição da República Portuguesa nos seus artigos 26º e 35º que consagram constitucionalmente a proteção de dados pessoais;
b) a Lei 43/2004 de 18 de Agosto – veio regular a Lei da Organização e Funcionamento da Comissão Nacional da Proteção de Dados;
c) a Lei 32/2008 de 17 de Julho – "transpõe para a ordem jurídica interna a Directiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações";
d) a Lei 67/98 de 26 de Outubro – Lei da Proteção de dados Pessoais – "transpõe para a ordem jurídica portuguesa a Directiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados";
e) entre outras.

Mas, uma vez que houve uma generalização desse desenvolvimento, surgiu a necessidade de uniformizar todas as normas estabelecidas em cada Estado - Membro

da União Europeia, sendo que deixaria de fazer sentido que cada um desses Estados tivessem a sua lei específica.

Nessa prespectiva, e depois de mais de quatro anos de discussões e diversas modificações, surge ,então, o "Regulamento Geral da Proteção de Dados da União Europeia". Assim, todas as regras foram uniformizadas em contexto comunitário, permitindo um maior controlo na proteção de dados.

Porém, fazendo uma breve referência ao que se aconteceu durante esses quatro anos que antecederam a publicação final e definitiva do Regulamento Geral da Proteção de Dados da União Europeia, temos:

- Primeiramente, a 7 de Dezembro de 2011 surge o primeiro rascunho das regras de proteção de dados da EU;
- De seguida, a 25 de Janeiro de 2012 foi publicado o projeto oficial do Novo Regulamento Geral de Proteção de Dados;
- A 7 de Março de 2012, a Autoridade Europeia para a proteção de dados deu o seu parecer face ao pacote de reforma de proteção de dados que foi emitido;
- A 20 de Março de 2012, o Parlamento Holandês aceitou a resolução pedindo ao governo que votasse contra o Regulamento de Proteção de Dados caso o nível de proteção de dados na regulamentação fosse menor do que o acto nacional de proteção de dados e, ao longo dos meses, foram vários os países que deram os seus pareceres face à elaboração do Novo Regulamento;
- A 3 de Maio de 2012, a Autoridade da Proteção de Dados da União Europeia emitiu uma resolução sobre a reforma da Proteção de Dados na Conferência da Primavera de 2012;
- Decorridos alguns meses, a 22 de Outubro de 2013 surge um novo artigo: "Regulamento da Proteção de Dados da União Europeia: Um passo à frente". A publicação deste artigo veio a revelar que existiam avanços nesta matéria, dando-a como certa a 12 de Março de 2014 após a esmagadora votação do Parlamento Europeu a favor das novas leis de proteção de dados.
- Assim, a 11 de Setembro de 2014 surge um novo artigo que comprova o caminho à reforma da proteção de dados: "10 recomendações para a reforma de dados da década";

- Por fim, a 15 de Dezembro de 2015, foi uma data decisiva, em que a Comissão Europeia, o Parlamento e o Conselho de Ministros chegou a acordo sobre o Regulamento Geral de Proteção de Dados, depois de vários meses de negociações; a 12 de Fevereiro de 2016 o Concelho da União Europeia confirmou o acordo face aos termos do Regulamento Geral da Proteção de Dados através de um acordo político sobre o mesmo e o Regulamento foi definitivamente adoptado a 14 de Abril de 2016;
- A 4 de Maio de 2016, o Regulamento Geral da Proteção de Dados foi publicado no Jornal Oficial da União Europeia, entrando em vigor 20 dias depois (25 de Maio de 2016) e terá um período transitório de dois anos para a sua total aplicação, sendo que todos os Estados – Membros terão esse período para se adaptarem às novas regras.

1.3. O Contexto do Regulamento Geral da Proteção de Dados da União Europeia

Ora, o Regulamento Geral da Proteção de Dados é aplicável aos 28 Estados Membros, assim sendo, não é necessária qualquer alteração na jurisdição de cada Estado, existindo, de facto, uma harmonização legislativa no que concerne à Proteção de Dados em todos os países da União Europeia.

O presente Regulamento (UE) 2016/679 vem, então, alterar radicalmente o quadro legal relativo à proteção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados e, desta forma, revoga a Diretiva 95/46/CE.

Face à já mencionada harmonização entre os Estados – Membros, este Regulamento dá especial ênfase à livre circulação dos dados permitindo um aumento significativo dos fluxos transfronteiriços de dados pessoais causado pela integração económica e social resultante do funcionamento do mercado interno.

O presente diploma vem ainda clarificar o conceito de dados pessoais e surgem também novos direitos para os titulares dos dados, como o direito à portabilidade dos dados; o direito ao esquecimento; e o direito de oposição e, traz também diversas adaptações em matéria de legalidade; obrigações dos responsáveis

de dados e subcontratantes; fiscalizações e sanções e proteções de dados em casos especiais.

No mesmo, foram também introduzidos novos princípios e conceitos como orientadores do tratamento dos dados como: *Privacy by design and by default* e a pseudonominação dos dados.

Ainda, em contrário do que acontecia com a Diretiva, este Regulamento é aplicável sobre os responsáveis pelo tratamento de dados, bem como, sobre os subcontratantes. Este aplica-se a tratamento de dados de titulares de dados pessoais Europeus, independentemente de o responsável pelo tratamento se encontrar ou não localizado na UE, segundo o artigo 3º do mesmo: ***"o presente regulamento 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".***

2. CONCEITOS BÁSICOS

2.1. O Conceito de Dados Pessoais

Como sabemos, o direito à proteção de dados pessoais advém de um dos direitos fundamentais do ser humano, consagrado na Declaração Universal dos Direitos do Homem, o direito à proteção da vida privada. Assim, uma vez que os nossos dados pessoais constituem informações da nossa vida privada, os mesmos devem ser, de facto, protegidos. Entende-se como vida privada tudo aquilo que esteja relacionado com a vida pessoal de cada um de nós. Não nos referimos apenas aos nossos dados mais íntimos mas também a dados da nossa vida profissional e social e esses, embora menos importantes, não devem ser esquecidos.

De acordo com a Diretiva nº 95/46/CE de 24 de Outubro, artigo 2º, alínea a), a definição de dados pessoais diz respeito a,

> ***"qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referencia a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".***

Assim, segundo orientação desta mesma Diretiva, também a Lei nº 67/98 de 26 de Outubro, no âmbito do seu artigo 3º, alínea a), dá uma definição para dados pessoais, definição essa bastante semelhante à apresentada anteriormente, em que, entende-se por Dados Pessoais,

> ***"qualquer informação, de qualquer natureza e independentemente do respectivo 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 directa ou indirectamente, 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".***

Também a Constituição da República Portuguesa refere, nos artigos 26º e 35º, o direito à vida privada e a proteção dos dados pessoais de cada ser humano. O artigo 26º da CRP (Outros direitos pessoais) menciona que,

> ***"A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação."***

Por sua vez, o artigo 35º da CRP (Utilização da Informática) refere que,

> ***"1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação 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 excepcionais 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 transfronteiriços e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional; Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei".***

Também o Regulamento Geral da Proteção de Dados da União Europeia, vem de alguma forma trazer um foco essencial no que diz respeito à definição de dados pessoais, presente no artigo 4º, nº1 do mesmo,

> ***««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, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular».

2.2. O Tratamento de Dados Pessoais

De acordo com o que está definido na Lei nº 67/98 de 26 de Outubro, primeiramente, o artigo 2º refere e muito bem que os dados devem ser tratados ***"de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais"***, sendo que o seu tratamento deve ser realizado com a maior seriedade e transparência perante o seu titular.

Ainda, o artigo 3º, alíneas a) e b) da mesma lei menciona que o tratamento de dados pessoais traduz-se numa ***"qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação ou interconexão, bem como o bloqueio, apagamento ou destruição"*** desses mesmos dados.

No presente regulamento, a definição de "Tratamento" aparece, no artigo 4º, nº2, um pouco diferente da da lei anteriormente mencionada, no entanto, são definições bastante semelhantes: ***"Tratamento, uma operação ou um conjunto de operações efetuadas sobre os dados pessoais ou sobre conjunto de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".***

No entanto, para que esses dados possam ser tratados, é necessário que a pessoa a quem os mesmos pertençam dê autorização para que isso aconteça, isto é, é necessário que o titular desses dados dê o seu consentimento, face ao tratamento dos mesmos. O seu consentimento é expresso de livre e espontânea vontade.

Analisemos, então, mais à frente o conceito de consentimento.

É, ainda, importante de referir que, no âmbito do artigo 35º da CRP, é garantido ao titular dos dados o direito a conhecer a finalidade dos seus dados. Cada uma das finalidades em causa dará lugar a diversos tratamentos específicos, que, por sua vez, deverão ser comunicados à entidade competente e, a falta de comunicação desse tratamento dará lugar ao incumprimento de obrigações da proteção de dados, ficando sujeito a uma multa até 120 dias, ou até um ano de prisão, no âmbito da Lei da Proteção de Dados, artigo 43º, nº1, alínea a).

Mas, e quem será esta entidade competente e que funções terá a mesma?

De acordo com o, ainda, artigo 35º, nº2, quando este refere a "entidade administrativa independente", esta surgiu em 1991 como a "Comissão Nacional de Proteção de Dados Pessoais Informatizados, instituída em 1994. No entanto, atualmente, e desde 1998, esta entidade é designada como "Comissão Nacional de Proteção de Dados".

Assim, a Comissão Nacional de Proteção de Dados (CNPD) é considerada como uma entidade administrativa independente e sobre ela recaem poderes de autoridade, junto da Assembleia da República. Esta, tem como principal função controlar e fiscalizar o processamento/ tratamento de dados pessoais, sendo que deve estar assegurado o respeito pelos direitos do Homem e pelas liberdades e garantias que se encontram consagradas na Constituição e na lei.

Esta Comissão é, também, considerada a Autoridade Nacional de Controlo de Dados Pessoais e é também responsável por cooperar com as autoridades de controlo de proteção de dados de outros Estados, zelando pela defesa e exercício dos direitos de pessoas que residam no estrangeiro, entre muitas outras competências. Qualquer decisão tomada pela CNPD tem força obrigatória, embora sejam passíveis de reclamar e recorrer.

Anteriormente à Revisão Constitucional de 1997, alguns tipos de dados não deveriam ser alvo de tratamento, com referência ao artigo 35º, nº3 da Constituição da República, assim como o artigo 7º, nº1 da Lei 67/98 de 26 de Outubro, sendo que estes mencionam a proibição do tratamento de dados que digam respeito a ***"convicções filosóficas ou políticas; filiação partidária; fé religiosa; vida privada e origem étnica e também dados relativos a saúde, vida sexual e dados genéticos".***

Estes dados, se tratados, podem revelar-se danosos, gerando uma eventual situação de discriminação. No entanto, após a Revisão de 1997, a lei passou a autorizar o tratamento desses dados, sob certas condições, como: se existisse garantia de não discriminação ou se o titular desses dados desse expressamente o seu consentimento.

Existem, ainda outros casos em que o tratamento de dados também é complexo, como o caso dos dados sensíveis, sujeito a um controlo e autorização por parte da CNPD, segundo o artigo 7º, nº2 da Lei 67/98, ***"mediante disposição legal ou autorização da CNPD, pode ser permitido o tratamento dos dados referidos no número anterior quando por motivos de interesse público importante esse tratamento for indispensável ao exercício das atribuições legais ou estatutárias do seu responsável, ou quando o titular dos dados tiver dado o seu consentimento expresso para esse tratamento, em ambos os casos com garantias de não discriminação e com as medidas de segurança previstas no artigo 15.º".*** Veremos este caso mais adiante.

Como referi na parte introdutória da minha dissertação, no Regulamento Geral da Proteção de Dados foram também introduzidos novos princípios e conceitos como orientadores do tratamento dos dados como: *Privacy by design and by default* e a pseudonominação dos dados.

Quanto à "*Privacy by design and by default"* este princípio define que as organizações devem ser capazes de demonstrar a sua conformidade com os princípios presentes no Regulamento Geral da Proteção de Dados, através da adopção de medidas adequadas de proteção de dados, consagrado no artigo 25º do RGPD com a epígrafe Proteção de dados desde a concepção e por defeito.

Desta forma, a "privacy by design", privacidade desde a concepção, significa que cada novo processo de negócios de serviços ou que faz uso de dados pessoais deve tomar a protecção desses dados em consideração, desde o início do seu "processo". Uma organização precisa ser capaz de mostrar que tem segurança adequada e que o seu cumprimento é realizado. Por seu turno, a "privacy by default", privacidade por padrão, significa que as configurações de privacidade mais rígidas se aplicam automaticamente, por defeito, quando um cliente adquire um novo produto ou serviço. Neste caso, as informações só serão guardadas durante o período necessário.

Assim, temos, segundo o disposto no artigo 25º:

1. ***"Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, …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, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares de dados;***
2. ***O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento… Em especial essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares".***

Por ultimo, quanto à Pseudonominação dos dados, esta é uma nova definição que consta do Regulamento Geral da Proteção de Dados, sendo que se refere a uma nova técnica de tratamento de dados pessoais, sendo que não são atribuídos dados específicos a um sujeito, substituindo o seu nome, bem como outras características de identificação, de forma a que seja impossível ou extremamente complicado de identificar a pessoa em causa e, assim, proteger a sua privacidade, de acordo com o artigo 4º, nº5, ***"Pseudonimização, 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".

Assim, podemos concluir que estas novas formas de tratamento de dados contribui para o cumprimento das regras de proteção da privacidade de cada ser humano.

2.3. O Conceito de Consentimento

O conceito de consentimento surge, então, na Diretiva 95/46/CE de 24 de Outubro, no artigo 7º ***"como um fundamento geral da licitude"***, sendo também interpretado ***"como um fundamento específico em certos contextos"***, segundo os artigos 8º, nº2, alínea a) e 26º, nº1, alínea a).

O consentimento por parte do titular dos dados é, de todo, necessário para o tratamento desses mesmos dados e este constitui apenas um dos seis fundamentos distintos que possibilitam a execução desse tratamento, segundo o artigo 7º da referida lei.

Ainda, no artigo 4º, nº11 do Regulamento Geral da Proteção de Dados, podemos encontrar uma definição bastante simples e explicativa do que se trata por consentimento: ***"Consentimento do titular de dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular de dados aceita, mediante declaração ou ato positive inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento".***

Analisando o artigo 8º da Diretiva mencionada, percebemos que o mesmo prevê a possibilidade do consentimento legitimar o tratamento, sendo proibido de outra forma, de categorias especiais de dados (sensíveis). Assim, tal como foi referido inicialmente, as regras para obtenção do consentimento por parte dos titulares tem um grau de exigência maior, sendo que este tipo de consentimento ultrapassa o grau normal de exigência.

O consentimento dos titulares para o tratamento dos seus dados prevê que possam ser evitados riscos face à divulgação inadequada da sua informação pessoal e

evita que sejam quebrados os direitos fundamentais dos indivíduos face à sua proteção.

Em conformidade com o desenvolvimento do direito fundamental à proteção de dados pelos tribunais superiores, o artigo 8º - Proteção de Dados Pessoais, da Carta dos Direitos Fundamentais vem comprovar esta visão:

> ***"1. Toda pessoa tem direito à proteção dos dados pessoais que lhe digam respeito;***
> ***2. Esses dados devem ser tratados leal, para fins específicos e com base no consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Toda pessoa tem direito de acesso aos dados coligidos que lhes digam respeito e o direito de ter a respectiva rectificação;***
> ***3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".***

Desta forma, este artigo da CDF permite o tratamento de dados pessoais apenas para fins específicos e com base no consentimento da pessoa interessada ou com outro fundamento legítimo previsto na lei. Assim sendo, o consentimento será sempre visto como um pilar fundamental no que toca à proteção de dados.

Ainda, o presente Regulamento esclarece e reforça a ideia de que qualquer consentimento deve ser expresso de forma explícita para que não hajam dúvidas face a essa matéria.

Assim, deixa de existir qualquer contradição entre o consentimento explícito e consentimento inequívoco. Em vez disso, este último aplica-se agora como um requisito geral para todas as situações que envolvam consentimento. O Regulamento Geral da Proteção de Dados abandona, então, este critério de distinção e agora, ao contrário da diretiva, de 1995, faz com que seja absolutamente claro que qualquer consentimento só pode ser expressa por meio de ação afirmativa clara. Além disso, o consentimento deve ser informado e livre, condições essas presentes no artigo 7º do mesmo.

3. NOVOS DIREITOS DO REGULAMENTO

Decorrentes do Regulamento Geral da Proteção de Dados surgem também novos direitos para os titulares dos dados, como: o direito à portabilidade dos dados; o direito ao esquecimento; e o direito de oposição. Para além destes, o RGPD prevê novos direitos individuais e reforça, também, alguns direitos já existentes no âmbito da legislação atual no que concerne à proteção de dados, como: o direito à informação, rectificação e eliminação, bem como deveres de informação e transparência. No futuro, a pessoa em causa pode esperar, acima de tudo, ser informado de forma mais abrangente e mais inteligível. Isso inclui receber informações significativas sobre a lógica envolvida em procedimentos automáticos para processamento de dados.

Analisemos, então, os três direitos referidos anteriormente.

3.1. Direito de Portabilidade de Dados

Relativamente ao direito à portabilidade dos dados, o Parlamento Europeu já havia mencionado o mesmo na Resolução de 2011, com o intuito de introduzir novas tecnologias mais conducentes à proteção de dados.

Este novo direito permitirá que os cidadãos transfiram com maior facilidade os seus dados de um prestador de serviços para outro. Isto é, o titular dos dados poderá levar os mesmos consigo para onde quer que vá. E, se facultou os seus dados a um determinado prestador de serviços e pretende mudar de prestador, então, o primeiro ficará obrigado a disponibilizar-lhe os seus próprios dados, através de um formato que possa ser facilmente transferido para o novo prestador.

Para que isso aconteça é, também, necessário que a tecnologia assim o permita. Como regra geral, a portabilidade dos dados deve ser assegurada de tal forma que os dados pessoais são comunicados à pessoa em causa em formatos electrónicos comumente utilizados, a fim de facilitar a sua futura utilização noutros contextos.

Assim, comprovando a existência do Direito de Portabilidade de Dados , o mesmo consta do artigo 20º, nº 1, alíneas a) e b) do Regulamento Geral da Proteção de Dados, que refere que ,

> ***"O titular de dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se: o tratamento se basear no consentimento dado nos termos do artigo 6º, nº1, alínea a) ou no artigo 9º, nº2, alínea a), ou num contrato referido no artigo 6º, nº 1, alínea b) e, se o tratamento for realizado por meios automatizados".***

3.2. Direito ao Esquecimento

O chamado "direito ao esquecimento" tem trazido diversas discussões no que diz respeito à sua aplicação prática.

Há relativamente pouco tempo, no ano 2014, ocorreu um caso bastante polémico face a esta matéria e a sua resolução levantou algumas questões pertinentes.

Mario Costeja González, cidadão espanhol, criou um anúncio no Jornal La Vanguardia sobre um leilão de imóveis para pagamento de dívidas à Segurança Social em que ele era um dos devedores. Fazendo uma pesquisa do seu nome na Google, o seu nome constava associado ao tal anúncio. Mario exigiu em tribunal que fosse eliminada a referência ao tal anúncio e o tribunal deu-lhe razão. No entanto, Mario queria também que o Jornal eliminasse o anúncio, no entanto, o tribunal não lhe deu razão, alegando que os meios de comunicação social estariam isentos desta decisão. Assim, se anteriormente este tipo de casos era susceptível de tremenda discussão, hoje, com o RGPD tudo se torna mais simples, na medida em que este novo direito ao esquecimento consta hoje no artigo 17º do Regulamento Geral da Proteção de Dados – Direito ao apagamento dos dados ("direito a ser esquecido"), ***"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" certos e determinados motivos, mencionados no mesmo artigo.

Assim, a eliminação desses dados é obrigatória, quando ocorrem as seguintes situações (artigo 17º, nº, alíneas a) a f)) :

> ***"a) quando os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;***
> ***b) quando o titular retira o consentimento em que se baseia o tratamento dos dados e quando não existe outro fundamento jurídico para o seu tratamento;***
> ***c) quando o titular se opõe ao tratamento e não existem interesses legítimos prevalecentes que o justifiquem; quando os dados pessoais foram tratados ilicitamente;***
> ***d) quando os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da UE ou de um Estado - Membro a que o responsável pelo tratamento esteja sujeito; e***
> ***f) quando os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação".***

Desta forma, podemos dizer que, sob determinadas condições, os cidadãos já têm direito a pedir, por exemplo, que os motores de busca suprimam ligações que conduzam a informações pessoais que lhes digam respeito, no entanto, como todos sabemos, e segundo o velho ditado, tudo é que é colocado na internet, dificilmente se apaga definitivamente...

Nesta prespectiva, o direito ao esquecimento impõe que o responsável pelo tratamento de dados disponha de meios que lhe permitam assegurar que os dados que lhe foram facultados pelo titular são, de facto, eliminados assim que o titular pretender, mesmo que esses dados tenham sido transmitidos a terceiros.

Ainda, não poderemos deixar de considerar que deve existir um equilíbrio entre o Direito ao Esquecimento e o Direito à Liberdade de Expressão, segundo refere o artigo 17º, nº3, alínea a) do RGPD, ***"os nºs 1 e 2 não se aplicam na medida em que o tratamento se revele necessário ao exercício da liberdade de expressão e de informação".***

Desta forma, poderemos dizer que o direito ao esquecimento tem, de facto, as suas excepções. De acordo com o artigo 17º, nº3, o mesmo não é viável quando estamos perante uma obrigação de exercício da liberdade de expressão e de informação; quando é exigível o cumprimento de uma obrigação legal face ao tratamento de dados, para exercício de funções de interesse público ou exercício da autoridade pública do responsável pelo tratamento; por motivos de interesse público no domínio da saúde pública; para questão de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos; para declaração, exercício ou defesa de um direito num processo judicial.

3.3. Direito de Oposição ao Tratamento de Dados

Ora, também em matéria de oposição ao tratamento de dados houve alguma inovação. Tendo em conta as novas disposições face ao tratamento automatizado de dados, o novo Direito de Oposição ao Tratamento de Dados encontra-se consagrado no artigo 21º do Regulamento Geral da Proteção de Dados. O mesmo diz-nos que

> ***" o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento de dados pessoais que lhe digam respeito com base no artigo 6º, nº1, alínea e) e f), ou no artigo 6º, nº4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento de dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular de dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial" (artigoº 21º, nº1).***

O indivíduo, pode ainda opor-se ao tratamento de dados se o propósito do processamento de dados ou perfil for considerado marketing direto, isto é, segundo o artigo 21º, nº2 do RGPD,

> ***"quando os dados forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao***

> ***tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta"***

E ainda, segundo o artigo 21º, nº3 do RGPD,

> ***"caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim".***

Para além disso, pela primeira vez, consta agora do artigo 19º do Regulamento, uma base jurídica face a novas normas técnicas no que concerne ao tratamento de dados, em caso de retificação ou eliminação de dados – Obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento: ***"o responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16º, artigo 17º, nº1 e o artigo 18º,salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento de fornece-lhe informações sobre os referidos destinatários".***

4. PRINCÍPIOS E LEGALIDADE DO TRATAMENTO DE DADOS

O Regulamento Geral de Proteção de Dados (que contém algumas leis aproximadas às leis alemãs de proteção de dados) tem agora um catálogo facilmente compreensível e claramente estruturado de princípios aplicáveis ao seu tratamento.

Como referi anteriormente, vou agora abordar cada um desses princípios.

Assim, o RGPD, no âmbito do seu artigo 5º, nº1, alíneas a) a f) com a epígrafe Princípios relativos ao tratamento de dados pessoais, menciona algumas regras que qualquer tratamento de dados pessoais deve obedecer:

a) o tratamento de dados deve ser lícito, justo e transparente, isto é, deve estar em conformidade com as normas estabelecidas na lei; de forma justa e clara– *"os dados pessoais são objecto de um tratamento lícito, leal e transparente em relação ao titular dos dados (licitude, lealdade e transparência)"*;
b) tem associada a recolha de dados de um determinado indivíduo, apenas para fins legítimos, específicos e explícitos – *"recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades,..."*;
c) deve ser limitado ao mínimo necessário em relação aos fins para os quais os dados são tratados – *"adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização de dados)"*; devem também ser concretos e devem ser atuais – *"exatos e atualizados sempre que necessário; devem ser adoptadas todas as medidas necessárias para os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (exatidão)"*;
d) devem também 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..." e,
e) devem ser protegidos de qualquer utilização inadequada e desrespeitante – *" 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 (integridade e confidencialidade)".*

Para além disso, deve também ser aplicado o princípio geral da responsabilidade pessoal, o que torna o processador inteiramente responsável por cumprir estes princípios e exige que o mesmo demonstre o cumprimento dos mesmos em todas as situações (artigo 24º do RGPD).

Todos estes princípios encontram-se também consagrados no âmbito do artigo 8º da Carta dos Direitos Fundamentais.

Outro desenvolvimento de grande importância face à matéria de princípios é que os mesmos, que estão mencionados no artigo 5º do RGPD, encontram-se também eles referidos ao longo de diversos pontos do Regulamento Geral da Proteção de Dados. Por exemplo, no RGPD agora existe um artigo específico sobre o conceito de proteção de dados desde a conceção, e por defeito – artigo 25º, artigo esse que colabora na aplicação dos princípios da proteção de dados obrigatórios para o responsável de dados. Também, como identificado no artigo 5º, a limitação da finalidade também constituiu um princípio do tratamento de dados, principio esse também mencionado no artigo 6º face à licitude do tratamento em termos de cumprimento de finalidades do mesmo.

4.1. Questão da Finalidade do Tratamento de Dados

Neste Novo Regulamento, existe agora um ponto muito importante no que concerne à referência a pseudónimos e à criptografia, consideradas como medidas de proteção de dados.

Assim, no âmbito do artigo 6º, nº3 do RGPD, poderemos encontrar uma forma mais concreta para definir a finalidade do tratamento de dados. Assim, segundo este artigo, **“ a finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no nº1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. ...”**

Desde a resolução de 2011 que o Parlamento Europeu defendia que não deveria haver alteração face ao nível de protecção e, em particular, portanto, a partir dos

princípios consagrados na diretiva de 1995, e por isso, foram rejeitadas várias propostas nesse sentido. Foi apenas aceite uma formulação específica do teste de compatibilidade.

4.2.Base jurídica para o Tratamento de Dados Pessoais

De acordo com o artigo 8º da Carta dos Direitos Fundamentais, para que o tratamento de dados pessoais seja lícito, é necessário garantir o consentimento do titular desses dados ou agir sobre qualquer outra regra imposta por lei.

Além disso, segundo o artigo 6º do Regulamento Geral da Proteção de Dados, são estabelecidos como elementos de autodeterminação da pessoa em causa cinco cenários em que o tratamento de dados é considerado lícito.

Assim, temos:

- o tratamento é lícito se "for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré – contratuais a pedido do titular dos dados(artigo 6º, nº 1, alínea b));
- se "for necessário o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (artigo 6º, nº 1, alínea c));
- se "for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular" (artigo 6º, nº 1, alínea d));
- se "for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento" (artigo 6º, nº 1, alínea e)); e,
- se "for necessário para efeito de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, excepto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança" (artigo 6º, nº 1, alínea f)).

4.3. O Interesse Legítimo

Embora o conceito de interesse legítimo já tenha sido debatido na diretiva de 1995, como uma base jurídica cada vez mais presente, este ganhou a sua especial importância no que concerne a uma das principais formas de conciliar de forma adequada os interesses dos consumidores e os interesses comerciais.

Esta matéria está, então, contemplada no artigo 6º do Regulamento Geral da Proteção de Dados (mencionado no ponto anterior), que deixa claro que a mesma não se aplica às transformações efetuadas pelas autoridades públicas no exercício das suas funções. Este artigo, reproduz ainda, amplamente, uma disposição equivalente à que se encontra na diretiva face à proteção de dados, com a exceção de que a necessidade de considerar especificamente os interesses e direitos das crianças consiste numa nova norma.

Na prática, face a essa inserção é provável que sejam necessários controladores para assegurar que qualquer decisão de processar os dados relativos às crianças, com base em interesses legítimos é cuidadosamente documentado e é realizada uma avaliação dos riscos envolventes e, os legítimos interesses não podem ser invocados pelas autoridades públicas em relação aos dados por eles tratados, quando exercício das suas funções.

Uma vez que esta questão foi deixada em aberto pela Comissão Europeia, na proposta de Janeiro de 2013 surgiram diversas situações de tratamento de dados em caso de crianças, sendo essas regularmente consideradas como interesses legítimos. Assim, devemos remeter-nos para a análise do artigo 6º, nº1 do Regulamento Geral da Proteção de Dados.

Face à proposta de Outubro de 2013, aprovada pelo Parlamento Europeu, essas situações foram reduzidas em larga escala, composta por vários pontos que as esclareciam, entre os quais o artigo 6º, nº1, alínea f) do RGPD – *"O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações.... o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou*

direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança".

5. ANÁLISE DAS OBRIGAÇÕES DOS RESPONSÁVEIS DE DADOS/ SUBCONTRATANTES

No que concerne às obrigações que devem ser cumpridas pelos processadores de dados/ Subcontratantes, existem algumas alterações significativas decorrentes do Regulamento Geral da Protecção de dados da União Europeia.

Assim, pela primeira vez, este Regulamento vem introduzir obrigações diretas aos processadores de dados, ao nível de toda a União Europeia. Tal permite que os titulares dos dados em tratamento possam fazer valer os seus direitos e asseguram a proteção da sua privacidade podendo, desta forma, intentar sanções contra os processadores de dados (multas possivelmente pesadas), caso ocorram situações de risco para os mesmos.

É importante referir que, tanto o responsável pelo tratamento de dados, como o subcontratante devem obedecer a determinadas regras, que se encontram agora consagradas no Regulamento: o responsável pelo tratamento porque é considerado, no âmbito do artigo 4º, ponto 7) do RGPD como uma,

> ***"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"***

Por sua vez, o subcontratante, no âmbito do artigo 4º, ponto 8) do RGPD, porque é considerado como uma

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

De acordo com o presente regulamento, existem diversos artigos que fazem menção à matéria das obrigações - artigo 24º e seguintes.

Para começar e, considerando que o tratamento de dados deve atender a certas exigências, a fim de assegurar ao titular dos dados que tudo corre bem, primeiramente, cabe ao responsável pelo tratamento implementar as medidas que considere adequadas, tendo em conta todos os aspectos que envolvam esse tratamento, garantindo que tudo decorre segundo as normas consagradas no presente Regulamento, podendo haver um reajuste das mesmas, conforme necessário – artigo 24º, nº1, do RGPD:

> ***"Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades".***

De acordo com o artigo 26º, nº1, do RGPD, quando se trata da envolvência de dois ou mais responsáveis pelo tratamento de dados, todos são responsabilizados pelo mesmo, assegurando o cumprimento de todas as suas responsabilidades perante o titular dos dados e os seus direitos:

> ***"quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento, Estes determinam, por acordo entre si e de modo transparente as respectivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que fiz respeito ao exercício dos direitos do titular dos dados e os respectivos deveres de fornecer as informações referidas nos artigos 13º e 14º..."***

Ainda, os responsáveis pelo tratamento de dados têm como tarefa nomear um subcontratante/ processador de dados que garanta a implementação de medidas técnicas e organizativas adequadas que comprovem o cumprimento dos requisitos impostos no Regulamento para a execução desse tratamento, artigo 28º, nº1 do RGPD:

> ***"quando o tratamento de 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".

De acordo com o artigo 29º do RGPD (Tratamento sob a autoridade do responsável pelo tratamento ou do subcontratante) percebemos que existe sempre uma relação entre o responsável do tratamento e o subcontratante, sendo que o processador dos dados/ subcontratante é obrigado a proceder ao tratamento de dados pessoais de um determinado titular de acordo com as instruções do responsável do tratamento:

"o subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento de dados ou do subcontratante, tenha acesso a dados pessoais, não procede ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados – Membros".

Como podemos constatar, segundo o artigo 32º do Regulamento Geral da Proteção de Dados, é adoptada uma abordagem bastante interessante no que diz respeito à segurança versus risco do tratamento de dados.

Assim, no ponto 1. do mesmo artigo, diz-nos que devem ser aplicadas, pelo responsável do tratamento, medidas adequadas com vista a garantir a segurança dos dados pessoais:

"Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:
a) a pseudonimização e cifragem dos dados pessoais;
b) a capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
c) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

d) um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento".

5.1. Violação de Dados

Decorrente de uma situação de insegurança dos dados, e caso haja uma violação dos mesmos, à necessário recorrer à autoridade de controlo para a resolução da situação em causa.

Assim, o artigo 33º e 34º do Regulamento Geral da proteção de Dados vem estabelecer alguns parâmetros a ter em conta nesse sentido como o dever de "Notificação de uma violação de dados pessoais à autoridade de controlo" e o dever de "Comunicação de uma violação de dados pessoais ao titular dos dados", respetivamente.

Quanto à Notificação da violação, cabe ao responsável pelo tratamento notificar tal situação à autoridade de controlo, até 72 horas após conhecimento da mesma, desde que tal violação não cause danos no que toca aos direitos e liberdades dos indivíduos:

"Em caso de violação de dados pessoais, o responsável pelo tratamento notificar desse facto a autoridade de controlo competente nos termos do artigo 55º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja susceptível de resultar num risco para os direitos e liberdades das pessoais singulares…"

Quanto à Comunicação da violação, o responsável do tratamento deve comunicar a mesma ao titular dos dados, sem demora injustificada, caso esteja inerente à mesma um elevado risco para os direitos e liberdades dos indivíduos:

" Quando a violação dos dados pessoais for susceptível de implicar um elevado risco para os direitos e liberdades das pessoais singulares, o responsável pelo tratamento comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada".

5.2. Avaliação de Impacto sobre a Proteção de Dados

Mais uma vez, o Regulamento Geral da Proteção de Dados, introduz uma nova norma e de extrema importância, na medida em que cria a possibilidade de ser avaliado o impacto que um determinado tratamento de dados, que implica um elevado risco para os direitos e liberdades dos indivíduos, pode originar. Tal norma mostrar-se, então, essencial, uma vez que, é possível evitar danos (graves), mesmo antes de se iniciar um processo de tratamento de dados, considerando que os mesmos podem causar graves consequências.

Assim, e em conformidade com o artigo 35º, nº1 do presente Regulamento, segundo a epígrafe Avaliação do impacto sobre a proteção de dados, temos:

> ***"Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a protecção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação."***

Embora países como a Alemanha e a Áustria tivessem votado a favor desta nova norma, a maioria mostrou-se contra esta exigência. No entanto, o Parlamento Europeu conseguiu chegar a acordo de que esta norma seria obrigatória em pelo menos três casos, com a exceção das normas estabelecidas nas leis dos Estados – Membros, que possam prever outros casos.

Assim, o artigo 35º, nº3 estabelece que a execução de uma avaliação de impacto sobre a proteção de dados é obrigatória em caso de:

> ***"a) Avaliação sistemática e complete dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizados, 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 9º, nº1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; ou***
> ***c) Controlo sistemático de zonas acessíveis ao público em grande escala."***

5.3. Códigos de Conduta e Certificação

Uma dos grandes pontos que também foi alvo de atenção, consagrado no Regulamento Geral da Proteção de Dados, foi a matéria relativa aos Códigos de Conduta e Certificação, presentes no mesmo, nos artigos 40º e 41º e nos artigos 42º e seguintes, respetivamente. O Regulamento pretende, então, esclarecer qual o papel que ambos desempenham face à lei da proteção de dados pessoais.

No âmbito dos artigos mencionados anteriormente, podemos encontrar uma enumeração de critérios de códigos de conduta e de certificação (artigos 40º e 42º) que nos remetem para um quadro legal obrigatório.

Quanto aos Códigos de Conduta, e de acordo com o artigo 40º, nº1 do RGPD, estes são elaborados por entidades competentes e têm como objectivo verificar que todos os parâmetros impostos pelo presente Regulamento são, de facto, cumpridos:

> ***"Os Estados – Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correcta aplicação do presente Regulamento, tendo em conta as características dos diferentes sectores de tratamento e as necessidades específicas das micro, pequenas e medias empresas."***

A criação, alteração ou aditamento de códigos de conduta é possível deste que sejam feitos por entidades competentes, com o intuito de especificar a sua aplicação no contexto do Regulamento em causa – artigo 40º, nº2:

> ***" As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente Regulamento."***

Por sua vez, no que diz respeito à Certificação, também ela é promovida pelas entidades competentes, sendo que são elaborados procedimentos de certificação no que concerne à proteção de dados, que podem levar, por exemplo, à atribuição de um selo europeu de proteção de dados – artigo 42º, nº1:

> ***"Os Estados – Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e medias empresas".***

Para além disso, e de acordo com o que é referido no artigo 42º, nº2, **"os procedimentos de certificação em matéria de proteção de dados... também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3º o quadro das transferências de dados pessoais para países terceiros ou organizações internacionais...".**

6. FISCALIZAÇÃO E SANÇÕES

Embora o processo legislativo tenha alcançado maior atenção em debates e negociações jurídicas, cujos mesmos incidiram em grande escala sobre as disposições face ao nível de proteção de dados e ao equilíbrio existente entre direitos e obrigações, talvez a parte que constituí maior importância do Regulamento Geral da Proteção de Dados é todo o mecanismo relativo à obrigatoriedade de cumprimento da lei, estando subjacentes as questões de fiscalidade e sanções, decorrentes dos artigos 51º e seguintes do presente Regulamento.

Toda e qualquer violação da lei, mas no caso particular, violação de dados pessoais, deve ser punida sendo que foge das regras legais que são imposta. A definição de "violação dos dados pessoais" está mencionada no artigo 4º, nº 12 como,

> ***"Violação de dados pessoais, uma violação da segurança que promove, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".***

Esta matéria já tinha sido apontada ,propositadamente, pelo Parlamento Europeu na sua resolução de 2011, não apenas com o intuito de atingir um nível elevado e uniforme de proteção de dados, com base na Diretiva 1995/46/CE, mas acima de tudo para uma melhor e maior uniformização da aplicação das disposições relativas à proteção de dados.

Assim, através da adopção deste novo regulamento geral e da sua interpretação coerente, além da sua aplicação obrigatória por meio de autoridades de controlo, que se certificarão de que todas as normas são cumpridas, foi possível alcançar uma utilização do E – Commerce cada vez maior, na sua generalidade, uma vez que as pessoas estão mais confiantes de que, quando colocam os seus dados à disposição, que os mesmos serão protegidos, bem como os seus direitos, tal como a sua privacidade e, por sua vez, foi possível alcançar uma igualdade de condições para que a proteção de dados prevaleça.

Neste contexto, as autoridades de controlo face à proteção de dados terão um papel fundamental no que concerne à garantia destas condições, perante todos.
Uma vez que se trata de um Regulamento Geral para toda a União Europeia, todos os Estados-Membros deverão, no futuro, chegar a acordo sobre uma abordagem coordenada e formular orientações comuns.

6.1. Autoridades de Controlo

Para que seja possível garantir a todas as pessoas singulares, a proteção dos seus dados pessoais, o desempenho das autoridades de controlo é fundamental. Nesse sentido, as autoridades de controlo têm como função fiscalizar e assegurarem de que tudo ocorre em consonância disposições legais do Regulamento Geral da Proteção de Dados da União Europeia.

Assim, a responsabilidade que as mesmas acarretam permite que seja verificada a aplicação dos direitos e liberdades fundamentais dos cidadãos e, por conseguinte, é possível zelar pela liberdade de circulação de dados na União – Artigo 51º, nº1 do RGPD.

> ***" Os Estados – Membros estabelecem que cabe a uma ou a mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União ("autoridades de controlo")".***

Inicialmente, o Parlamento Europeu mencionou que tal seria possível de funcionar se, em caso de litígio, as autoridades de controlo se comprometesses a seguir uma linha comum vinculativa face a uma decisão da maioria. Mais tarde, este ponto de vista foi, então, aceite pelo parlamento Europeu e pelo Conselho de Ministros da União Europeia. Segundo o mesmo, "qualquer decisão transfronteiriça relevante sobre um caso individual tomada por uma autoridade pode agora, sob certas condições, ser aplicada por todas as outras autoridades de supervisão para fins de resolução de litígios". Isto é, tal irá contribuir para que haja uma coerência na

aplicação de normas em toda a união e assim, seguirem uma linha comum, como referido anteriormente. Segundo o artigo 51º, nº3 do RGPD temos,

> ***"Quando estiverem estabelecidas mais do que uma autoridade de controlo num Estado – Membro, este determina qual a autoridade de controlo que deve representar essas autoridades no Comité e estabelece disposições para assegurar que as regras relativas ao procedimento de controlo de coerência referido no artigo 63º, sejam cumpridas pelas autoridades".***

Assim, se analisarmos o que nos diz o referido artigo 63º do RGPD, percebemos que existe, de facto, uma relação "solidária" entre as autoridades e, por vezes, a própria comissão, zelando pela aplicação uniforme das normas impostas no presente Regulamento, decorrentes da ordem jurídica de todos os Estados – Membros, garantindo a máxima eficácia da proteção jurídica.

> ***"A fim de contribuir para a aplicação coerente do presente Regulamento em toda a União, as autoridades de controlo cooperam entre si e, quando for relevante, com a Comissão, através do procedimento de controlo da coerência previsto na presente ação".***

E ainda, o artigo 51º, nº2 reforça essa ideia:

> ***"As autoridades de controlo contribuem para a aplicação para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de controlo cooperam entre si e com a Comissão, nos termos do Capítulo VII" (Cooperação e Coerência).***

Geralmente, a competência de cada autoridade de controlo de protecção de dados é determinada tendo em conta a sua localização, no território do seu Estado – Membro da União Europeia. No entanto, podem ocorrer transferências de dados pessoais para países terceiros ou organizações internacionais e, nesse caso, o Capítulo V do Regulamento Geral da Proteção de Dados Pessoais da União Europeia, vem impor disposições legais para legislar essas situações.

Assim, para que não exista qualquer risco associado a uma possível transferência de dados para países terceiros é necessário cumprir todas as disposições presentes no mencionado Capítulo do RGPD.

Primeiramente, e segundo o artigo 44º do RGPD,

> ***"Qualquer transferência de dados pessoais que sejam ou venham a ser objecto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento".***

Ainda, no artigo 45º, nº1, o Regulamento faz, novamente, referência a que, essa transferência transfronteiriça só é possível se a Comissão decidir que a mesma não trará qualquer perda de segurança face à proteção dos dados transferidos para países terceiros:

> ***"Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais sectores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica".***

Para tal, a Comissão procede a uma avaliação do nível de proteção que um determinado país terceiro demonstra ter, de acordo com os parâmetros estipulados no artigo 45º, 2.

Assim, segundo o artigo 46º com a epígrafe Transferências sujeitas a garantias adequadas, são enumeradas diversas garantias que devem ser verificadas para que seja possível proceder transferência de dados.

Em suma, existem ainda transferências que não são permitidas, pelo direito da União. Desta forma, segundo o artigo 48º, ***"As decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento ou o subcontratante transfiram ou divulguem dados pessoais só são reconhecidas ou executadas se tiverem como base um acordo internacional, como***

um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados – Membros, sem prejuízo de outros motivos de transferência nos termos do presente capítulo".

Concluindo a referência às transferências entre países terceiros, de acordo com o artigo 50º do RGPD, existe uma preocupação por parte da Comissão e das autoridades de controlo no que concerne à proteção de dados pessoais, isto é, ambas elaboraram entre si medidas que devem ser cumpridas pelos países terceiros ou organizações internacionais de forma a que a segurança desses dados prevaleça intacta:

> ***"Em relação a países terceiros e a organizações internacionais, a Comissão e as autoridades de controlo tomam as medidas necessárias para:***
>
> ***a) Estabelecer regras internacionais de cooperação destinadas a facilitar a aplicação efectiva da legislação em matéria de proteção de dados pessoais;***
> ***b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à protecção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, e assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;***
> ***c) Associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais;***
> ***d) Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, nomeadamente no que diz respeito a conflitos jurisdicionais com países terceiros."***

É ainda de salientar que, para além de tudo aquilo que já foi mencionado anteriormente, também o Comité representa uma imagem importante em todo este contexto, na medida em que, também ele pode dar o seu parecer nesta matéria, em casos em que a autoridade de controlo tenha de adotar determinadas medidas que devem ser analisadas por uma entidade superior, o Comité.
Tal acontece, de acordo com o artigo 64º, nº1, quando a autoridade de controlo:

> ***a) Vise a adoção de uma lista das operações de tratamento sujeitas à exigência de proceder a uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35º, nº4;***

b) Incida sobre uma questão, prevista no artigo 40º, nº7, de saber se um projeto de código de conduta ou uma alteração... está em conformidade com o presente regulamento"
... Entre outras."

6.2. Sistema de Sanções e Coimas

O sistema de sanções identificado no Regulamento Geral da Proteção de Dados da UE constitui, também ele, um fator de grande importância no que diz respeito às inovações que este novo regulamento trouxe, principalmente no que toca aos atores economicamente mais fortes que operam internacionalmente, uma vez que, são esses atores que mais transação de dados provocam pela sua diversidade de negócios e comércio por todo o Mundo.

Assim, o regime de sanções está previsto no presente regulamento, no Capítulo VIII, Vias de recurso, responsabilidade e sanções.

De forma a reforçar o cumprimento das novas regras estabelecidas pelo presente regulamento, os países da União Europeia terão de impor sanções, incluindo coimas, ou aplicar medidas que sejam adequadas, impostas pelas autoridades de controlo.

Segundo o artigo 84º do RGPD, com epígrafe Sanções, temos:

"Os Estados – Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 83º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas".

Quanto à aplicação de coimas, o Regulamento Geral da Proteção de Dados estipula que, em caso de uma violação das regras legais do mesmo, as coimas são impostas para além ou em vez de outras medidas que a autoridade de controlo pode aplicar, segundo o artigo 58º, nº2, alíneas ***"a) fazer advertências ao responsável do***

tratamento ou ao subcontratante no sentido de que as operações de tratamento tiverem violado as disposições do presente regulamento"; "h) retirar a certificação ou ordenar ao organismo de certificação que retire a certificação..." e j) ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais", conforme referido no artigo 83º, nº2.

Assim, todas as coimas impostas devem ser eficazes em todo o seu âmbito, aplicadas de acordo com cada caso específico.

Veremos agora, dois casos concretos relativos à aplicação obrigatória de coimas.

6.2.1. Incumprimento de Obrigações

Segundo o artigo 83º, nº4, caso haja violação das seguintes obrigações,

> ***a) As obrigações do responsável pelo tratamento ou subcontratante nos termos dos artigos 8º, 11º, 25º a 39º e 42º e 43º;***
> ***b) As obrigações do organismo de certificação nos termos dos artigos 32º e 43º;***
> ***c) As obrigações do organismo de supervisão nos termos dos artigos 41º, nº4,***

é aplicada uma coima ***"até 10 000 000 Eur ou, no caso de empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior...".***

Assim, é estabelecido um parâmetro distinto entre a aplicação de coimas a particulares e a empresas.

6.2.2. Violação de princípios e direitos e incumprimento de ordens impostas pela de controlo

No caso em que não sejam cumpridas as disposições legais, e por isso violados os princípios, os direitos individuais das pessoas em causa e as regras respeitantes a transferências de dados pessoais para um país terceiro; ou ainda, for violada uma ordem imposta pela autoridade de controlo, o limite superior para tal coima é nesse

sentido aumentado para um máximo de 4% do volume de negócios anual mundial, caso se trate de uma empresa, ou até € 20 milhões, em casos particulares.

Assim, segundo o artigo 83º, nº5,

> ***" A violação das disposições a seguir enumeradas está sujeita, em conformidade com o nº2, a coimas até 20 000 000 Eur, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:***
> ***a) os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5º, 6º, 7º e 9º;***
> ***b) os direitos dos titulares dos dados nos termos dos artigos 12º a 22º;***
> ***c) as transferências de dados pessoais para um destinatário num país terceiro ou numa organização internacional nos termos dos artigos 44º a 49º;***
> ***d) as obrigações nos termos do direito do Estado – Membro adotado ao abrigo do capítulo IX;***
> ***e) o incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58º, nº2, ou o facto de não facultar acesso, em violação do artigo 58º, nº1".***

E, ainda, de acordo com o artigo 83º nº6,

> ***"O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58º, nº2, está sujeito, em conformidade com o nº2 do presente artigo, a coimas até 20 000 000 Eur ou, no caso de uma empresa, até 4% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado".***

7. PROTEÇÃO DE DADOS ESPECIAL

O Regulamento Geral de Proteção de Dados estabelece algumas disposições especiais, em determinadas situações face ao processamento de dados ou dá aos Estados – Membros ou ao legislador da União Europeia autonomia para agir. Veremos, então, alguns casos especiais face à matéria em causa.

7.1. Dados Sensíveis

O caso mais importante no que concerne à proteção de dados especial é o caso dos dados sensíveis. Esta matéria, para além de já estar prevista na Diretiva de 1995, está mencionada no artigo 9º do RGPD. O tratamento deste tipo de dados é, geralmente, proibido, embora possa ser permitido em determinadas circunstâncias.

Assim, segundo o artigo 9º, nº1 do mesmo, ***"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 para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"*** é proibido, isto porque são dados de extrema intimidade e que, se conhecidos por pessoas alheias podem originar diversos problemas para a pessoa em causa.

Face à legislação já existente em relação a esta matéria, talvez a alteração mais relevante aqui presente é a inclusão de dados biométricos para efeitos de identificação e dados genéticos na lista de dados sensíveis, sendo que ambos se encontram definidos no âmbito do artigo 4º, nº 14) e 13), respetivamente,

> ***"Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" e,***
>
> ***"Dados genéticos, os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta***

designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa".

De seguida, no ponto 2 do artigo 9º, encontramos as disposições em que o tratamento de dados sensíveis é permitido. Assim, para além dos casos em que a pessoa em causa consente explicitamente, temos os casos em que o tratamento desses dados é necessário para "***efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação labora; segurança social;.."*** (alínea b)); é necessário para ***"proteger os interesses vitais do titular dos dados ou de outra pessoa singular"*** (alínea c)); é necessário para o ***"âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação;..."*** (alínea d)); entre outros.

7.2. A Proteção de Dados de Menores

Desta vez, face a outro domínio da proteção de dados em regime especial, também o Regulamento destaca uma grande evolução, no que concerne à proteção especial dos dados pessoais de crianças (nomeadamente em casos em que esses dados servem para comercialização ou criação de perfis;...).

Tanto a Comissão Europeia como o Parlamento Europeu pretendiam estipular um limite de idade face ao consentimento de crianças para o tratamento dos seus dados.

Assim, no âmbito da sociedade da informação, o tratamento de dados de crianças só é viável se as mesmas tiverem pelo menos 16 anos. Caso tal não aconteça, é necessário que haja consentimento dos pais para que se proceda ao tratamento desses dados, artigo 8º, nº1, o tratamento de dados pessoais de crianças ***"... é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança".***

No entanto, os Estados-membros da UE podem dispor no seu direito uma idade inferior, com uma idade limite mínima de 13 anos. Para isso, o responsável pelo tratamento terá de verificar que o consentimento foi dado ou autorizado.

É, ainda, importante referir que todo o consentimento deve ser dado de forma clara e explícita para que não haja dúvidas do mesmo.

Com a impossibilidade de manter limites de idade entre 16 e 18, completamente irrealistas, em vigor, foi finalmente acordado que os Estados-Membros devem definir um limite nacional entre 13 e 16 anos, acima do qual as crianças seriam capazes de lançar de forma independente os seus dados pessoais , incluindo no âmbito dos serviços da sociedade da informação.

Transpondo toda esta matéria para a realidade, há muito pouco tempo, ou seja, no passado dia 12 de Outubro de 2016, foi publicado pelo Jornal Público um artigo de toda a importância, referente ao tema aqui a ser tratados, cujo tema do mesmo era " Escolas não podem mostrar dados pessoais de alunos na Net", trazendo para discussão questões de "**divulgação de informação em *sites* abertos. Publicação de fotografias e vídeos de alunos em ambiente escolar suscita "as maiores reservas" da Comissão Nacional de Protecção de Dados".**

Sobre esta matéria, a Comissão Nacional da Proteção de Dados vem condenar as Escolas pela sua prática no que toca a "divulgar dados pessoais dos alunos nos *sites* das escolas, como as pautas com as classificações, imagens dos menores e os horários lectivos. E alerta para os riscos que esta publicação traz para essas crianças e jovens, nomeadamente para a sua segurança".

Tais dados são considerados pela mesma como possíveis "juízos estigmatizantes com elevado potencial discriminatório" ou permitir a um criminoso saber a hora a que uma criança sai da escola".

Uma vez que se tratam de dados bastante pessoais e, por isso, muito delicados, a Comissão lança algumas orientações concretas a escolas públicas e privadas, dirigidas a todos os anos escolares com o intuito de sensibilizar todos para a gravidade da questão. Tal necessidade de orientação deve-se ao facto de haver inúmeras queixas por parte dos pais face a esta realidade, sendo que já foram aplicadas coimas a muitas escolas.

Segundo Clara Guerra, porta voz da CNPD, A exposição pública dos dados dos menores detidos pelas escolas "é altamente violadora da privacidade e tem um impacto muito significativo na vida atual e futura dos alunos".

Segundo a Comissão, as Escolas, enquanto "instituições" que devem "proteger ativamente os seus alunos e respeitar os seus direitos fundamentais", não podem permitir que situações como estas aconteçam. É natural que a internet seja vista como um meio de fácil acesso a informações e é, por isso utilizada no seu âmbito, no entanto, "a exposição pública dos dados dos menores detidos pelas escolas é altamente violadora da privacidade e tem um impacto muito significativo na vida atual e futura dos alunos".

Existe, de facto, uma gravidade extrema, uma vez que, como todos podem aceder à internet, em qualquer parte do Mundo, esses dados correm o risco de serem copiados e utilizados de forma inadequada e, certamente, que tal situação trará consequências severas para as crianças em causa. Para além de que, como referida pela CNPD, a divulgação desses dados pedem resultar, por sua vez, na divulgação de "informação relativa a uma pessoa singular, identificada ou identificável".

Deve, portanto, existir uma grande preocupação face à proteção da informação que é divulgada e, no caso da publicação de pautas nas escolas, existem sites de acesso reservado que pode ser utilizado para esse fim que, segundo a Comissão, está "sujeita a mecanismos rigorosos de autenticação de utilizadores devidamente autorizados". Mas insiste que cada encarregado de educação só deve ter acesso aos dados do aluno que tutela".

A CNPD alerta ainda para os perigos da informação dispersa, que apesar de não ter o nome dos alunos, pode ser cruzada com outros dados permitindo, por exemplo, perceber qual é o horário de uma determinada criança".

Concluíndo, podemos dizer que não basta que seja a Comissão a criar orientações e chamadas de atenção severas. Cada um de nós deve ser capaz de se proteger, proteger a divulgação dos seus dados pessoais e, acima de tudo, deve proteger a privacidade das crianças, uma vez que existem situações que podem por em risco a própria vida das crianças e, por vezes, tais situações não são perceptíveis

para os menores. Assim, cabe aos adultos zelar por essa segurança.

Sem dúvida, um tema cada vez mais visível na nossa atualidade.

7.3. Abordagem de cada Estado - Membro

Embora o objectivo fundamental do Regulamento Geral da Proteção de Dados seja encontrar disposições legais relativas à proteção de dados pessoais que sejam aplicadas de uma forma uniforme face a todos os Estados – Membros, o presente Regulamento prevê algumas situações em que os próprios Estados – Membros têm a possibilidade de impor as suas próprias regras, daí entender tal como mais um caso especial de proteção de dados.

Desta forma, podemos referir o exemplo de, tentar conciliar a protecção de dados do titular de dados com o direito à liberdade de expressão e liberdade de imprensa e de informações onde são referidas disposições decorrentes de ordenamentos jurídicos do direito dos próprios Estados-Membros, uma vez que não existem padrões mínimos para a liberdade dos meios de comunicação aplicáveis em toda a UE – artigo 80º do RGPD, ***" O titular de dados tem o direito a mandatar um organismo, organização... que esteja devidamente constituído ao abrigo do direito de um Estado – Membro..."***.

Desta forma, a intenção não é desligarmo-nos dessa uniformização mas sim dar alguma motivação a que os Estados – Membros possam ganhar alguma "margem de manobra" a fim de poderem instituir o seu direito interno. O objectivo é que os Estados – Membros possam também eles impor as suas regras, desde que tal não quebre a harmonização que se está a tentar criar no contexto da União Europeia.

8. PRESPETIVAS PARA O FUTURO/ CONCLUSÕES

Como podemos constatar, o Regulamento Geral da Proteção de Dados da União Europeia vem a demonstrar um papel tremendamente importante no que concerne à imposição de uma maior segurança jurídica face à proteção de dados pessoais e desta forma, tal trará enormes vantagens face à utilização crescente do E – Commerce. Assim, a elaboração e prática do presente regulamento marcará, com toda a certeza, um longo mas importante caminho a percorrer face à aplicação de regras que são impostas no âmbito de toda a União Europeia, a fim de estabelecer uma uniformização de normas e uma harmonização entre todos os Estados – Membros, regulando, desta forma, todo o "mercado digitalizado e globalizado" que é o E – Commerce, criando total confiança neste novo conceito e cumprindo todos os direitos fundamentais da União Europeia.

Com a entrada em vigor deste novo regulamento, e de acordo com as novas disposições legais contempladas no mesmo, será possível encarar todos os desafios legislativos que possam surgir, decorrentes da "Era Digital", de uma forma mais simples e de fácil resolução, havendo agora uma base jurídica claramente mais sólida do que aquela que existia anteriormente.

Como já era de prever, o Regulamento Geral da Proteção de Dados da UE veio trazer uma nova visão face ao Mundo tecnológico. Houve uma mudança significativa, sendo que já existem empresas que utilizam este novo modelo europeu de proteção de dados, principalmente aquelas que utilizam a internet como um meio de informação e comunicação com o Mundo e, por isso, uma vez que este Regulamento veio transmitir uma maior confiança face à segurança na utilização do E – Commerce, as mesma já começam a usufruir das vantagens que daí advém.

"Além disso, por meio de suas novas disposições legais da UE está também a estimular a tomada de decisão política noutros outros países. O debate sobre a proteção dos dados dos consumidores nos EUA vai ser revigorada, e a abordagem dos

europeus, que se baseia em princípios e direitos fundamentais, também terá de ser tida em conta nos acordos internacionais, por exemplo, sobre o livre comércio".

Face a este Regulamento, considero que as expectativas futuras são bastante risonhas uma vez que, acredito que o mesmo trará muitas vantagens para todos, sendo que estamos perante um crescimento económico global, em que todas as empresas mas também todos os utilizadores poderão usufruir desta nova "Era". Temos um mercado em expansão, haverá um aumento significativo no volume de negócios, a economia está a ser estimulada e em crescimento exponencial, não esquecendo, contudo, que tudo será um grande desafio para todos.

É necessário cumprir com todas as novas disposições legais impostas neste novo Regulamento pela União Europeia, e é necessário, também, que haja uma interpretação coerente do mesmo entre todos os Estados – Membros. Se tal acontecer, tudo será muito mais simples e tudo funcionará da melhor forma.

Neste Contexto, podemos referir que, embora a criação deste novo regulamento seja um passo fundamental para a formulação de uma visão uniforme de um mundo digital, tal irá, certamente, permitir constituir um marco na integração Europeia, em que todos os Estados – Membros se unem por uma União Europeia mais forte e mais resistente a todos os desafios que terá de ultrapassar. Assim, o surgimento do presente Regulamento constitui, de facto, um momento essencial e fundamental na integração e uniformização da União Europeia.

Concluindo, posso dizer que o desenvolvimento todo este trabalho foi bastante interessante e superou todas as expectativas, na medida em que desenvolvi um tema que se encontra na atualidade e que, ao longo do tempo irá, certamente suscitar o interesse de todos uma vez que, demonstrará num futuro breve, com toda a certeza, muitas evoluções no decorrer do tempo.

No futuro, acho que seria interessante pensar neste tema ainda mais evoluído, chegando a um contexto, não só Europeu, onde já se encontra, mas Mundial. Era

interessante conseguir conciliar o "Mundo" num só caminho, a sua globalização e uniformização.

10. REFERÊNCIAS BIBLIOGRÁFICAS

- ASENSIO, Pedro Alberto de Miguel – Derecho Privado de Internet, 5ª Edição, Thomson Reuters, Civitas, p. 291 – 377;
- Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro, 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
- FERREIRA, Pedro – A Protecção de Dados Pessoais na Sociedade de Comunicação: Dados de Tráfego, Dados de Localização e Testemunho de Conexão. Lisboa: O Espírito das leis editora, Lda. 2006. 455 p. ISBN 978-9020-13-2;
- HEIMES, Rita, "Top 10 operational impacts of the GDPR; Part 1 – data security and breach notification", The Privacy Advisor, Westin Research Center;
- HUMPHREYS, Matthew & HORSPOOL, Margot – European Union Law, 8ª Edição, Ed. Oxford;
- Lei nº 67/98 de 26 de Outubro – Lei da Proteção de Dados Pessoais;
- a Lei 43/2004 de 18 de Agosto – Lei de organização e funcionamento da Comissão Nacional de Proteção de Dados;
- a Lei 32/2008 de 17 de Julho – Conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações electrónicas;
- MARTINS, Ana Maria Guerra – Manual de Direito da União Europeia. 2014, Almedina Editora;
- PHILIPP, Jan – Article: "The EU´s New Data Protection Law – How A Directive Evolved Into A Regulation", CRi magazine, pag. 33-43;
- PINHEIRO, Alexandre de Sousa – Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional. Lisboa: AAFDL, 2015;
- REED, Chris – Computer Law, 7ª Edição, Oxford Editora;
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);

- Revista de Direito Intelectual Nº2, 2015, Almedina;
- RODRIGUES, Benjamim Silva – Constituição da República Portuguesa, 1ª Edição (Atualizada), Rei dos Livros Editora, 2011;
- WAELDE, Edwards and Charlotte – Law and the Internet, BLOOMSBURY PUBLISHING PLC Editora, 2009;
- WEIGL, Michaela – Article: "The EU General Data Protection Regulation´s Impacto on Website Operators and eCommerce", CRi magazine, 4/2016.