O REGULAMENTO GERAL DA PROTEÇÃO DE DADOS NO ÂMBITO TECNOLÓGICO

THE GENERAL DATA PROTECTION REGULATION IN THE TECHNOLOGICAL FIELD

Hélio Lameiras[1]

Resumo

A globalização e a rápida evolução tecnológica vieram dar origem a incontáveis atividades que envolvem diariamente o processamento e circulação de dados pessoais. A utilização dessas informações por parte de entidades públicas ou privadas, deve obedecer a um conjunto de procedimentos que permitam o cumprimento das novas normas de proteção de dados contempladas no novo Regulamento Geral da Proteção de Dados (RGPD). Este artigo centra-se na problemática da proteção de dados pessoais, prestando particular atenção às novas medidas legais, técnicas e organizacionais no âmbito tecnológico.

PALAVRAS CHAVE: RGPD, Dados pessoais, Titulares de dados, União Europeia; EPD, Responsável do tratamento de dados, Subcontratante, Autoridades de Controlo, CNPD; Avaliação de impacto sobre os dados.

Abstract

Globalization and rapid technological evolution have given rise to countless activities that daily involve the processing and circulation of personal data. The use of this information by public or private entities must follow a set of procedures that allow compliance with the new data protection rules contemplated in the new General Data Protection Regulation (GDPR). This article focuses on the issue of personal data protection, paying particular attention to new legal, technical and organizational measures in the technological field.

KEYWORDS: RGPD, Personal data, Data subjects, European Union; EPD, Data controller, Subcontractor, Supervisory Authorities, CNPD; Data impact assessment.

1. INTRODUÇÃO

A sociedade atual dispõe de uma conectividade tecnológica como nunca antes vista, permitindo de uma forma rápida e eficaz desenvolver um vasto leque de atividades diárias, públicas ou privadas, suportadas por plataformas tecnológicas desenhadas para o devido efeito. Muitas destas atividades requerem o tratamento de dados pessoais, as quais utilizam a tecnologia existente para

[1] hlameiras@ipcb.pt; Instituto Politécnico de Castelo Branco

a sua rápida recolha, processamento e armazenamento. Embora considerado um aspeto positivo, a disponibilidade existente e em muitos casos o fácil acesso a estes dados, originam situações em que os mesmos são tratados para fins diferentes do inicialmente previsto.

Muitas situações problemáticas têm surgido, desde a simples utilização do email pessoal para fins de marketing não autorizado até situações mais gravosas como o roubo de identidade, fraude bancária, branqueamento de capitais e terrorismo. Muitos Estados trocam diariamente informações financeiras de uma forma automática, com o intuito de combater grande parte destes problemas, especialmente na evasão e elisão fiscal abusiva, pois é de seu interesse a manutenção da integridade do seu sistema fiscal, obtendo as necessárias receitas para a consecução dos seus fins (Pichel, 2018).

Os titulares deparam-se com os seus dados pessoais mais expostos, perdendo em muitos casos o controlo sobre os mesmos, dando origem a uma violação dos seus direitos mais fundamentais. Face a este problema cada vez mais complexo, agravado pelo rápido avanço da tecnologia, a União Europeia (UE) elaborou um novo regulamento para proteger os seus cidadãos, revogando a anterior Diretiva 95/46/CE[2] pelo Regulamento Geral de Proteção de Dados (RGPD), o qual entrou em vigor a 25 de maio de 2018, reforçando os direitos já conferidos e o controlo dos titulares sobre os seus dados pessoais, impondo novas regras e obrigando as organizações a implementar processos e procedimentos conformes o RGPD (Fazendeiro, 2017).

Desta forma surge um novo quadro legal, promovendo mudanças consideráveis no setor empresarial, de acordo com a sua dimensão e natureza, área de atividade e tipo de tratamento dos dados pessoais que realizem.

Através do RGPD, a UE pretende contribuir para o bem-estar das pessoas singulares, da sua segurança e justiça, bem como para uma união económica que promova a consolidação e a convergência das economias a nível do mercado interno. O RGPD destina-se ao tratamento de dados pessoais realizado em qualquer país da UE e não exclui qualquer tipo de suporte, seja em papel, eletrónico, informático, som e imagem ou outro (Sousa, 2018).

Este novo regulamento embora imponha às organizações a obrigação de preservar a privacidade dos dados, os titulares também deverão contribuir igualmente para a sua própria privacidade. Embora conscientes dos riscos, muitas das vezes os titulares trocam as suas informações pessoais por descontos em supermercados, aceitando termos e condições sem lê-los, o mesmo acontecendo na utilização das redes sociais (Presthus, 2018).

Para os titulares de dados, conhecer o novo RGPD significa conhecer os seus direitos e também os comportamentos de segurança que devem adotar.

2. DADOS PESSOAIS

Considerando o artigo 3.º do RGPD, entende-se por dados pessoais a "*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 eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*". Tudo o que possa identificar um indivíduo engloba-se nesta definição, nomeadamente: nome, morada, data de nascimento, NIF, imagens e sons relativos à pessoa, recolhidos através de qualquer sistema de videovigilância, gravação telefónica e endereços de IP.

Da tutela da reserva da vida privada, existem dados que pelas suas características únicas e muito específicas são chamados de 'dados sensíveis', pertencentes à esfera mais íntima da pessoa, cujo tratamento pode expor e causar danos consideráveis ao titular. Falamos de dados que revelam a

[2] Diretiva 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 de dados pessoais e à livre circulação desses dados.

origem racial ou étnica, convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, dados genéticos e biométricos, bem como dados relativos à saúde e à vida sexual, cujo tratamento passou também a ser proibido. Comparando o artigo 8.º, n.º 1 da revogada Diretiva 95/46/CE, esta proibição foi positivamente ampliada a estes dados pelo RGPD, imperando a opção legislativa aos Estados-Membros de poderem regulamentar a proteção destes dados (Sousa, 2018). Podemos ainda destacar os dados pessoais de saúde, que incluem toda a informação relativa à saúde de uma pessoa e que são utilizados pelos profissionais de saúde na sua relação assistencial, recolhidos por observação clínica ou exames laboratoriais, categorizados pela sua natureza e registados nos processos clínicos. Estes dados originam um historial clínico que não é do conhecimento apenas de um profissional de saúde, mas sim de uma equipa multidisciplinar (Deodato, 2017). Face a esta realidade, ao longo dos anos e por uma questão de tratar da sua saúde ou de outras situações, o titular expõe constantemente os seus dados, mas com o direito a que estes estejam devidamente protegidos.

3. HARMONIZAÇÃO LEGISLATIVA NO ESPAÇO EUROPEU

Com a entrada em vigor do Tratado da UE, vieram beneficiar das liberdades comunitárias todos os nacionais dos Estados-Membros. O estatuto de cidadão da UE tende a ser o estatuto fundamental dos nacionais dos Estados-Membros, os quais obtêm o mesmo tratamento jurídico, permitindo desta forma que estes circulem livremente no espaço europeu, residindo, respondendo a ofertas de emprego, prestando ou adquirindo bens e serviços (Gorjão-Henriques, 2005).

O projeto europeu procura constantemente melhorar o seu funcionamento, proteger o seu espaço e garantir os direitos dos seus cidadãos, necessitando de criar ou atualizar as suas linhas de orientação frequentemente. Com os resgates ao setor financeiro ocorridos na crise de 2007, a UE evidenciou ocultações de património e obtenção de rendimentos à margem dos sistemas fiscais, passando desde essa época a adotar instrumentos de troca automática de informações financeiras, segundo uma norma comum. Estes instrumentos determinam a troca em massa de informação, que vai além do espaço da União, integrando-se num sistema global com grande amplitude objetiva e subjetiva (Pichel, 2018). O RGPD é também um desses instrumentos, cujo objetivo se prende com harmonização de toda a legislação relacionada com a proteção de dados pessoais em toda a UE.

O RGPD no seu âmbito, protege os cidadãos europeus dentro das suas fronteiras, mas também fora delas, pois só é realizado o tratamento de dados pessoais europeus num país terceiro ou organização internacional se forem respeitadas as condições estabelecidas nele por parte do responsável do tratamento e subcontratante. A Comissão Europeia é que decide se o país terceiro, território ou organização internacional assegura um nível de proteção adequado para que sejam feitas as transferências de dados (artigo 44.º e 45.º do RGPD).

4. PRINCIPAIS VIOLAÇÕES TECNOLÓGICAS DE DADOS

Grande parte dos dados pessoais são processados e armazenados em sistemas computacionais, os quais devem estar devidamente protegidos com políticas de segurança, garantindo o acesso apenas a utilizadores autorizados e com operações de recuperação e restauro em caso de falha física dos equipamentos tecnológicos.

No entanto, esta realidade não é tão fácil de gerir quanto se pensa, pois por mais bem elaborado que seja o plano de segurança da rede informática, podem surgir situações não previstas que comprometam o sistema e os dados pessoais. Além destas situações não previstas, existe sempre o perigoso risco das atividades não autorizadas, as quais podem ter origem em dois universos populacionais disjuntos: os sujeitos com privilégios acrescidos pertencentes à organização detentora

do sistema computacional que se pretende proteger e os que a ela não pertencem (Zúquete 2018).

A rapidez com que se aderiu aos sistemas informáticos e à Internet, quer seja no meio empresarial ou doméstico, levou a que uma grande quantidade de computadores e redes protegidas ficassem à mercê de atacantes espalhados pelo mundo inteiro.

Um estudo levado a cabo pela empresa internacional de segurança digital denominada Gemalto, refere que só no primeiro semestre de 2018 foram comprometidos cerca de 3,4 biliões de registos de dados. Através da Figura 1, podemos analisar as principais fontes e tipos de violações de dados.

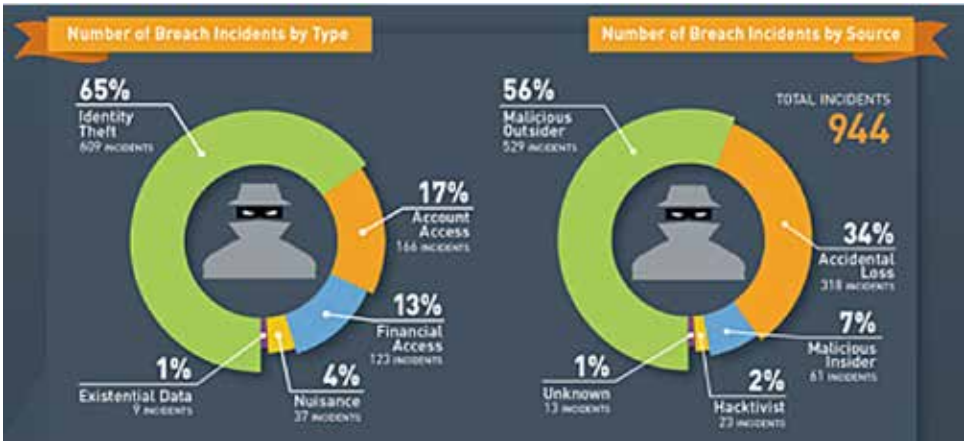

Figura 1 – Tipos e fontes das principais violações de dados. Fonte: Gemalto (2019).

Na Figura 1, verificamos que nas violações por tipo, o roubo de identidade assume o maior destaque (65%) seguido dos acessos indevidos a contas (17%). Os problemas causados pelo roubo de identidade podem levar meses ou anos a solucionar, pois as vítimas necessitam de provar que não foram os executantes das ilicitudes, acrescendo o facto de não saberem a quantidade de atividades ilícitas praticadas com os seus dados.

O artigo 15º da Lei 10/91, refere que os dados pessoais só podem ser utilizados para a finalidade determinante da sua recolha, logo atividades não autorizadas ou não realizadas pelo titular tais como a utilização de acessos digitais roubados em compras online são consideradas atividades ilegais e uma das mais conhecidas. A utilização de cartões de crédito roubados para gastos diversificados, aberturas de contas para branqueamento de capitais, fraude fiscal e acesso indevido aos locais que o titular normalmente tem autorização exclusiva, são outros dos exemplos de atividades ilícitas bastante lesivas para o titular que podemos destacar e refletir sobre tudo o que poderá suceder negativamente.

A Figura 1 permite-nos verificar também que no caso das violações por fonte, os agentes externos maliciosos (56%) e as perdas acidentais (34%) são os mais frequentes. Os agentes externos identificam-se normalmente por Hackers[3] ou outros agentes externos automatizados com os mesmos objetivos. Os Hackers, na maioria das vezes, partilham informações entre si, originando grupos com uma cultura própria, ideologia e motivações particulares, capazes de realizar atividades focadas no roubo de dados pessoais a larga escala para depois serem utilizados em atividades terroristas, derrube de regimes ou organizações.

Apesar das organizações estarem cientes dos dados sensíveis que guardam e de realizarem boas práticas de segurança na proteção dos mesmos contra Hackers, é um facto que a corrupção ou eliminação desses dados bem como as perdas acidentais provocadas pelos utilizadores são também

[3] Indivíduos que se dedicam de uma forma intensiva a conhecer e modificar o normal funcionamento de equipamentos e programas em redes informáticas para proveito próprio, utilizando os seus conhecimentos de programação para fins ilícitos.

uma das situações mais preocupantes, pois essas perdas de informação sensível originam na maioria dos casos prejuízos substanciais (Zelenay, 2019).

TYPE OF BREACH	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Identity Theft	6,152,772	1,183,250,626	320,301,914	215,270,492	180,902,284	337,957,794	318,340,752	79,160,614	323,454,199	621,276,348	2,772,437,893
Financial Access	4,088,747	270,371,346	34,905,015	117,209,547	1,200,098	2,943,207	2,147,030	2,374,097	2,708,295	22,669,150	388,100,303
Account Access	498,291,533	111,487,991	50,941,357	918,530,886	89,681,373	82,191,718	175,606,078	154,592,156	84,045,984	819,877,277	219,945,423
Nuisance	2,664,521	26,159,788	19,539,907	8,421,285	15,592,468	268,354	168,483,495	72,245,792	1,543,884,696	47,990,745	1,694,029
Existential Data	2,060,093	3,529,008	2,963,243	383,174	21,284,089	4,000,309	451,955	415,008,711	425,284	7,586	11
TOTALS	513,197,666	1,594,768,751	428,651,436	2,459,815,384	316,101,112	427,361,462	665,009,310	723,181,380	1,952,669,358	1,511,021,106	3,353,172,708

Figura 2 – Número de violações de dados por tipo. Fonte: Gemalto (2019).

Na Figura 2 podemos comparar a evolução do número de violações entre o ano de 2013 e 2018. No roubo de identidade verificamos que no primeiro semestre de 2018 os números de violações foram superados em mais de 2 biliões relativamente ao primeiro semestre de 2013. É verdadeiramente preocupante esta realidade, pelo que as boas práticas de segurança e a consciencialização desta realidade devem ser fortemente difundidas.

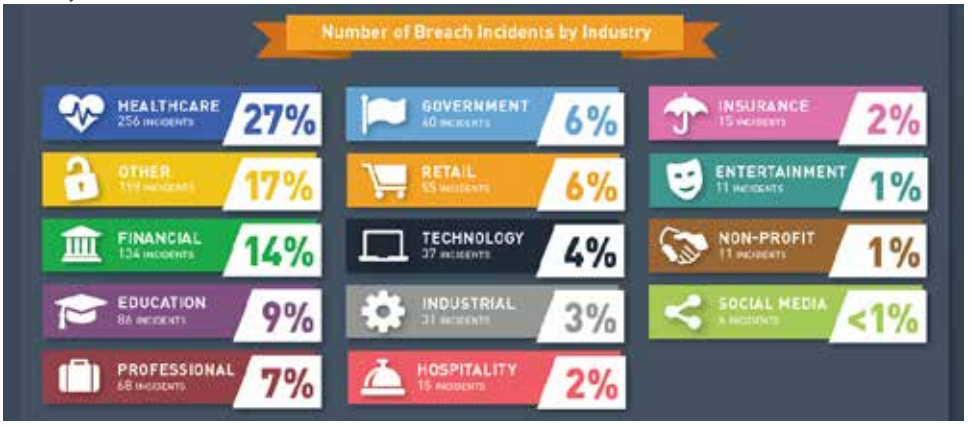

Figura 3 - Violações de dados por setor de atividade. Fonte: Gemalto (2019).

Se tivermos em conta os setores de atividade apresentado na Figura 3, o que apresenta maior destaque é o ramo da saúde (27%), no qual existem muitos dados pessoais sensíveis, anteriormente destacados. Estes dados pessoais podem ser utilizados para uma enorme quantidade de atividades ilícitas, nomeadamente saber o estado de saúde de uma pessoa para de alguma forma prejudicar o mesmo, quer seja a nível laboral, físico ou simplesmente a nível de imagem. Normalmente os mais visados são as figuras públicas e elementos que ocupam cargos importantes, aos quais são feitas chantagens a fim de obter dinheiro, favores ou vantagens concorrenciais sob ameaça de revelar a sua situação de saúde.

Segundo Zúquete (2018), as atividades ilícitas podem-se encaixar em cinco tipos-base:

- Acesso a informação;
- Alteração de informação;
- Utilização exagerada ou abusiva de recursos computacionais;
- Impedimento de prestação de serviço;
- Vandalismo.

São diversas as atividades ilícitas, mas as principais categorizam-se em: agentes externos maliciosos[4], perdas acidentais, hacktivistas[5], agentes maliciosos internos[6], patrocinados estatais e desconhecidos.

BREACH SOURCE	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Malicious Outsider	902,709,483	1,578,575,971	359,090,929	1,569,453,283	175,545,401	99,259,842	569,960,152	687,888,769	261,894,208	491,540,648	2,448,160,927
Accidental Loss	8,468,082	6,702,567	4,771,897	305,300,000	33,977,717	231,236,930	258,763,768	33,498,745	1,660,677,295	529,347,310	879,628,507
Hacktivist	777,216	98,799	7,000,096	1,182,007	961,918	30,011,304	11,495,895	918,179	70,000	1,784	13,215,237
Malicious Insider	1,160,667	9,221,729	108,770,712	74,968,030	2,006,460	62,785,175	19,484,124	489,497	80,227,855	191,966	12,163,866
State Sponsored	88	166,016	3,016,499	606,912,064	104,009,225	4,047,411	10,355,381	442,200	0	0	0
Unknown	72,780	4,745	1,307	0	391	200	350,000	0	0	0	4,171
TOTALS	913,197,666	1,594,768,751	426,651,436	2,459,815,384	316,101,112	427,361,462	669,009,310	723,181,330	1,953,669,358	1,011,021,106	3,353,172,708

Figura 4 - Número de violações de dados por tipo. Fonte: Gemalto (2019).

Estas atividades têm vindo a aumentar de ano para ano como podemos confirmar na Figura 4. Só de atividades maliciosas externas, entre o primeiro semestre de 2013 e 2018, assistimos a um aumento perto dos 500% na violação de registos.

Perante esta realidade podemos verificar que estes tipos de atividades ilícitas certamente não irão abrandar, muito pelo contrário, serão cada vez mais agressivas, dotadas de ferramentas e procedimentos especializados para cometerem os seus crimes, levando a cabo as suas verdadeiras intenções lesivas, comprometendo milhões de dados pessoais. A estas atividades ainda acresce o problema de existirem dispositivos conectados à Internet com segurança limitada ou inexistente, facilitando a monitorização de comunicações, permitindo acessos e utilizações indevidas a qualquer tipo de informação privada (Allhoff, 2018).

De forma a controlar estas atividades ilícitas, em cada Estado-Membro da UE existe uma ou mais autoridades públicas independentes criadas pelo mesmo nos termos do artigo 51º do RGPD.

4.1. Autoridades de Controlo

Tendo em conta a problemática da violação de dados anteriormente mencionada, existem as autoridades de controlo cuja finalidade será a de controlar essa situação, analisando as reclamações que a si são feitas bem como a fiscalização da aplicação do RGPD. Pretende desta forma defender os direitos e liberdades das pessoas singulares relativamente ao tratamento de dados e a sua livre circulação na UE. Os membros das autoridades de controlo não solicitam nem recebem instruções de outrem, pelo que não estão sujeitos a influências externas, diretas ou indiretas no seu desempenho de funções (artigo 51.º e 52.º do RGPD).

Um dos maiores destaques que o RGPD apresenta, é o aumento substancial das coimas por incumprimento, as quais podem ascender a € 20.000.000 ou a 4% da faturação anual no caso das empresas. Os dados pessoais que são um direito do homem, passam agora a ser identificados como um "Corporate Risk"[7] (Fazendeiro, 2017).

Em Portugal, existe atualmente uma entidade administrativa independente com poderes de autoridade denominada Comissão Nacional de Proteção de Dados (CNPD), a qual funciona junto da Assembleia da República, cuja função é o controlo e a fiscalização do processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na Lei.

[4] Elementos externos à entidade detentora do sistema computacional que contem os dados pessoais.
[5] Pessoas ou grupos que recorrem a crimes cibernéticos para promover uma ideologia política, crenças, interesses ou ideais.
[6] Elementos internos que pertencem à entidade detentora do sistema computacional que contem os dados pessoais.
[7] Risco corporativo, o qual deve ser devidamente gerido e protegido para evitar perdas financeiras

5. TRATAMENTO DE DADOS

De acordo com o artigo 3.º do RGPD, entende-se por tratamento de dados, como sendo "*uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição*". Desta forma, considera-se tratamento de dados quaisquer operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não. As principais operações que podemos categorizar são:

- Recolha;
- Registo;
- Organização;
- Estruturação;
- Conservação;
- Adaptação ou alteração;
- Recuperação.

Também é considerado como tratamento de dados a eliminação ou destruição de dados, a consulta, a divulgação, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização (Guerra, 1997).

5.1. Consentimento

Todas as atividades realizadas que envolvam processamento de dados, estão agora mais protegidas devido ao novo regulamento, pois será sempre necessário dar o consentimento para o respetivo tratamento. Se isso não ocorrer estamos perante uma ilegalidade. O consentimento é considerado pelo artigo 4º do RGPD como sendo "*uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*".

A licitude do tratamento de dados está sobretudo ligada às obrigações ou autorizações que o titular de dados consentir. Podemos referir que é lícito quando verificamos pelo menos uma das seguintes situações (artigo 6.º do RGPD):

- O titular de dados tiver dado o seu consentimento para uma ou mais finalidades específicas;
- O tratamento seja necessário para a celebração de um contrato de um ou mais indivíduos;
- O tratamento seja necessário para o cumprimento de uma obrigação jurídica;
- O tratamento seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- O tratamento seja necessário ao exercício de funções de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento.

Muitos formulários web apresentam campos de preenchimento de dados que vão além do estritamente necessário para o tratamento. No caso de existirem opções pré-validadas ou omissas, não se pode confirmar o consentimento por parte do titular de dados, pois todas as atividades realizadas durante o tratamento devem ser o mais claro e transparentes possíveis, para que se saiba especificamente a finalidade e evitar tratamentos múltiplos não consentidos. O titular dos dados

tem o direito de retirar o seu consentimento a qualquer momento, pois este deve ser tão fácil de retirar quanto de dar (artigo 7.º do RGPD).

Menores de 16 anos

Desde a nascença que qualquer indivíduo adquire direitos e deveres, ou seja, personalidade jurídica e dados pessoais. Embora titulares, em Portugal até aos 16 anos, são os responsáveis parentais que autorizam ou não o tratamento dos seus dados, uma vez que as crianças requerem atenção especial devido ao facto de estarem menos cientes dos riscos, consequências e direitos relacionados com o tratamento dos seus dados pessoais. Alguns Estados-Membros da UE podem legislar uma idade inferior para os menores, desde que não seja inferior a 13 anos (artigo 8.º do RGPD).

Nos dias de hoje, os menores de idade estão rodeados de tecnologia e na maioria das vezes utilizam-na. O simples facto da sua utilização para entretenimento ou realização de atividades escolares, implica em muitos casos aceitar um conjunto de termos e condições do fabricante do software ou hardware, nomeadamente jogos ou aplicações de diversos tipos.

Perante esta situação, os responsáveis parentais têm a seu cargo uma tarefa mais complicada em educar as crianças e a supervisão das suas atividades, acrescendo o problema que nem eles próprios às vezes conhecem como funciona realmente determinada tecnologia e as implicações que a sua utilização acarreta.

5.2. Responsável pelo Tratamento de Dados, Subcontratantes e Encarregado de Proteção de Dados.

No tratamento de dados existem normalmente vários intervenientes sobre os quais recai a responsabilidade do tratamento. Estes devem desde o início desenvolver procedimentos no tratamento que permitam garantir a segurança dos dados pessoais e assegurar que se destinam a ser processados mediante a finalidade definida em concordância com o regulamento e a autorização do titular de dados. De acordo com o artigo 3.º do RGPD, podemos definir como responsável pelo tratamento de dados, "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

O responsável pelo tratamento deve apresentar as medidas técnicas e organizativas apropriadas, de forma a assegurar que o mesmo é realizado em conformidade com o RGPD. Os responsáveis pelo tratamento de dados e o seu representante, se existir, devem conservar um registo completo de todas as atividades de tratamento sob a sua responsabilidade, os nomes dos responsáveis, as finalidades do tratamento, o prazo previsto para a eliminação, entre outras informações.

Tanto no momento de definição dos meios de tratamento como no próprio tratamento, o responsável deve aplicar as medidas técnicas e organizativas adequadas, tais como a pseudonimização[8] e minimização[9] necessários para cada finalidade específica do tratamento. Devem ser sempre incluídas as garantias necessárias no cumprimento do RGPD bem como a proteção dos direitos dos titulares de dados, tratando-se apenas os dados necessários para as finalidades definidas.

[8] 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.

[9] Tratamento de dados pessoais que sejam apenas estritamente necessários, relevantes e adequados ao fim específico.

Figura 5 – Etapas de um tratamento de dados. Fonte: Elaboração própria.

A proteção de dados é um processo que desde a sua fase de conceção deverá adotar medidas de *Privacy by Design*, as quais segundo (Cavoukian, 2011) são fundamentais para a proteção de informações privadas existentes na era moderna. O mesmo refere que a privacidade deve ser parte integrante das prioridades organizacionais, dos objetivos de projeto, de design e operações de planeamento, bem como ser incorporada em todos os padrões, protocolos e processos que afetam as nossas vidas. Estas medidas podem-se dividir em sete princípios fundamentais:

- Medidas proativas e não reativas, evitando eventos invasivos de privacidade antes que eles aconteçam;
- Privacidade através da utilização de regras padrão;
- Privacidade embebida no desenho;
- Funcionalidade total, sem comprometer a segurança;
- Segurança fim-a-fim (como um ciclo);
- Visibilidade e transparência;
- Respeito pela privacidade do utilizador.

No caso de existir mais do que um responsável pelo tratamento de dados, ambos devem determinar entre si de uma forma transparente, quais as responsabilidades de cada um no cumprimento das suas funções de acordo com o RGPD. Ambos devem conhecer as orientações e finalidades do tratamento, de forma a esclarecer ou fornecer informações acerca do ponto de situação do tratamento ao titular dos dados. Cada vez que o titular necessitar de tomar uma decisão relativamente ao tratamento, este deve ser previamente e suficientemente informado de todas as implicações (O´Conner, 2017).

O responsável do tratamento de dados pode recorrer a um subcontratante para realizar o tratamento de acordo com a estratégia idealizada, no entanto o subcontratante não pode contratar outro sem autorização do responsável do tratamento por contrato escrito. De acordo com o artigo 3.º do RGPD, entende-se por subcontratante, "uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Todo o tratamento de dados tem associado a si um determinado grau de risco, pelo que deve ser bem analisada a sua quantidade a nível regional, nacional ou supranacional. Caso afetem um

número considerável de titulares de dados e o tratamento seja considerado de grande escala, é obrigatório a nomeação de um Encarregado de Proteção de Dados (EPD), bem como se o tratamento for realizado por uma autoridade ou organismo público ou estiver relacionado com condenações penais e infrações. A principal função de um EPD é assegurar o cumprimento do RGDP, assessorando o responsável pelo tratamento ou o subcontratante. Este deverá primar pelos seus conhecimentos especializados, qualidade e sigilo profissional, dotado de integridade e ética, detendo conhecimentos da legislação em matéria de proteção de dados. O EPD não recebe instruções relativamente às suas funções, poderá acumular outras funções e nunca poderá ser destituído pelo responsável do tratamento de dados (artigo 37º e 38º do RGPD).

As atividades de todos estes agentes devem ter como linha de orientação o RGPD, mas torna-se necessário encontrar um ponto de equilíbrio com o mesmo para que não prejudiquem o negócio da organização sempre que existir alguma inconformidade.

5.3. Segurança e Avaliação de Impacto sobre a Proteção de Dados

Perante as potencialidades da conectividade tecnológica atual, os dados pessoais estão sujeitos a maiores riscos. Tendo em conta a sua natureza, âmbito, contexto e finalidades, sempre que exista um risco elevado para as liberdades das pessoas singulares, o responsável pelo tratamento deverá realizar antes de iniciar o tratamento, uma avaliação de impacto das operações sobre a proteção de dados. Esta será obrigatória sempre que se produzam efeitos jurídicos relativamente à pessoa singular baseada no tratamento automático, bem como operações de tratamento em grande escala de categorias especiais de dados e controlo sistemático de zonas acessíveis ao público em grande escala (artigo 35º, n.º 1 e n.º 2 do RGPD).

A avaliação de impacto é desta forma um processo que avalia a necessidade do tratamento, descrevendo o mesmo a sua proporcionalidade, riscos e medidas preventivas.

Figura 6 - Processo de uma avaliação de impacto sobre a proteção de dados. Fonte: Elaboração própria.

Esta avaliação deverá incluir pelo menos uma das seguintes opções: descrição sistemática das operações do tratamento previstas e a finalidade do mesmo; uma avaliação da necessidade e proporcionalidade das operações; uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos; medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais (artigo 35º, n.º 7 do RGPD).

O responsável do tratamento e subcontratante devem garantir que o EPD está envolvido precocemente na avaliação de impacto e devidamente informado de todas as questões da proteção de dados. O EPD deve ser informado e consultado desde o início das avaliações de impacto sobre a proteção de dados, bem como este deve ser interlocutor interno e externo da organização. Também deverá ser convidado regularmente para participar nas reuniões dos quadros de gestão médios e superiores das organizações, pois só assim com toda esta envolvência poderá tomar decisões e pareceres adequados.

Os responsáveis do tratamento de dados podem criar códigos ou aditações, mas são obrigados sempre a apresentá-los à autoridade de controlo, a qual emitirá um parecer consoante o seu conteúdo. O cumprimento de códigos de conduta ou de procedimentos de certificação aprovados pode ser utilizado como elemento para comprovar o cumprimento das obrigações do responsável pelo tratamento.

6. CÓDIGOS DE CONDUTA

Atendendo às necessidades específicas das micro, pequenas e médias empresas, são elaborados de Códigos de Conduta que contribuem para a correta aplicação do RGPD. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão são os responsáveis por promover a elaboração dos mesmos. A supervisão destes códigos pode ser feita por um organismo acreditado para o efeito. Desta forma, os Estados-Membros devem promover a criação de condutas de certificação em matéria de proteção de dados, bem como selos e marcas para efeitos de comprovação da conformidade das operações de tratamento de dados (artigo 40.º e 41.ºdo RGPD).

As obrigações dos responsáveis do tratamento de dados e dos subcontratantes, podem ser reguladas pelos códigos de conduta, tendo em atenção o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas.

7. CONSIDERAÇÕES FINAIS

Por toda a europa trabalhou-se intensamente e foram feitas revisões das leis nacionais de proteção de dados para ter ser possível a concretização e aplicação do RGPD de forma a aumentar a proteção dos dados pessoais dos cidadãos europeus. A harmonização de toda a legislação relacionada com esta proteção de dados no espaço europeu veio responder a uma crescente problemática relacionada com o roubo de dados pessoais ou utilização indevida dos mesmos.

Assume um grande destaque no RGPD a obrigatoriedade de reportar a uma autoridade de controlo qualquer problema relacionado com falhas de segurança assim como o registo de todas as atividades relacionadas com o tratamento e o devido consentimento por parte do titular de dados para um tratamento específico. A definição de responsabilidades e principais funções dos diversos elementos que realizam o tratamento bem como a necessidade de ser criada toda a documentação para comprovar o tratamento é também uma mais-valia. O não respeito por este regulamente permite às autoridades de controlo aplicar coimas que atingem valores muito significativos, demonstrando que este assunto deverá ser encarado com seriedade.

Existe agora um regulamento atualizado que confere uma maior proteção dos dados pessoais, mas isso não significa que os titulares de dados possam descansar relativamente à sua segurança. Anteriormente referimos as principais violações atuais de dados no âmbito tecnológico e verifi-

camos que as atividades ilícitas irão continuar a crescer e a adotarem técnicas mais agressivas até atingirem os seus fins. Um cidadão europeu responsável deverá conhecer o RGPD e proteger os seus dados adotando comportamentos seguros na utilização da tecnologia existente.

Este regulamento é certamente um instrumento muito importante na defesa dos dados pessoais, mas com a crescente evolução tecnológica irão surgir novos desafios, levando o mesmo a evoluir e adaptar-se às novas realidades de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

Allhoff, F. e Henschke, A. (2018). Internet of Things: Foundational ethical issues. *Internet of Things*, 1-2, pp. 55-66.

Cavoukian, A. (2011). *Privacy by Design, The 7 Foundational Principles*. Acedido a 9 de novembro de 2019, em https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Deodato, S. (2017). *A proteção dos dados pessoais de saúde*. Lisboa: IDG – Imagem Digital Gráfica, Lda.

Fazendeiro, A. (2017). *Regulamento Geral sobre a Proteção de Dados.* Braga: Papelmunde-Sociedade de Manufacturas Gráficas, Lda.

Gemalto (2019). *Data Privacy and New Regulations Take Center Stage - First Half Review* 2018. Acedido a 9 de novembro, em https://www.thalesesecurity.com/2019/data-threat--report

Gorjão-Henriques, M. (2005). *Direito Comunitário*. Coimbra: C.C. – Gráfica de Coimbra, Lda.

Guerra, A. (1997). *Informática e Tratamento de Dados Pessoais*. Lisboa: Vislis Editores, Lda.

O´Connor, Y., Rowan, W., Lynch, L. e Heavin, C. (2017). Privacy by Design: Informed Consent and Internet of Things for Smart Health. *Procedia Computer Science*, 113, pp. 653-658.

Pichel, P. (2018). Troca automática de informações financeiras, respeito pela vida privada e proteção de dados pessoais. *Fórum de Proteção de Dados*, 5, pp. 30-59.

Presthus,W. e Sorum, H (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. *Procedia Computer Science*, 138, pp. 603-611.

Sousa, I. (2018). Do respeito pela vida (relativamente) privada no âmbito da videovigilância. *Fórum de Proteção de Dados*, 5, pp. 60-71.

RGPD (2016). *Jornal Oficial da União Europeia*. Acedido a 9 de novembro de 2019, em http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN

Zelenay, J., Balco, P. e Gregus, M. (2019). Cloud technologies – solution secure communication and collaboration. *Procedia Computer Science*, 151, pp. 567-574.

Zúquete, A. (2018). *Segurança em Redes Informáticas*. Lisboa: FCA – Editora de Informática, Lda.