Notificações de violações de dados:

a mudança de paradigma com o regulamento geral de proteção de dados

Graça Maria Neves Pacheco Costa

Dissertação para obtenção do Grau de Mestre em

Segurança de Informação e Direito no Ciberespaço

Orientadores: Professor Doutor Carlos Caleiro

Professora Doutora Luísa Neto

Professora Doutora Filipa Calvão

Júri

Presidente: Professor Doutor Paulo Mateus

Orientadora: Professora Doutora Filipa Calvão

Vogal: Professor Doutor Luís Antunes

Dezembro de 2018

Resumo

As violações de dados são incidentes de segurança que evidenciam a colisão com o direito fundamental à proteção de dados (cf. n.º 1 do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia e n.º 1 do artigo 16.º do Tratado sobre o Funcionamento da União Europeia), que merecem uma abordagem própria.

Estando consciente desta problemática, o legislador europeu verteu esta preocupação no novo quadro legislativo da proteção de dados pessoais, acentuando a responsabilidade e a transparência. Nesse sentido, uma das principais inovações do Regulamento Geral de Proteção de Dados (Regulamento (UE) 2016/679, doravante RGPD) consiste na obrigação de os responsáveis pelo tratamento de dados pessoais notificarem as autoridades competentes – e nalguns casos, os titulares de dados afetados – relativamente a determinadas violações de dados pessoais.

Todavia, pese embora o RGDP contenha algumas diretrizes quanto a estas notificações no que concerne ao prazo, à autoridade de controlo competente, aos casos em que é também necessário notificar os titulares dos dados afetados, e às consequências da não notificação, etc. (cf. Artigos 33.º e 34.º do RGPD), este diploma é omisso quanto às comunicações internas e externas necessárias para a deteção, reporte, mitigação de efeitos adversos, com vista a que a notificação de violações de dados pessoais ocorra dentro do prazo de 72 horas após a tomada de conhecimento das mesmas pelo responsável pelo tratamento.

É para tal reflexão sobre as notificações de violações de dados que este trabalho pretende contribuir, buscando-se a definição de linhas gerais de ação, boas práticas e cadeias de comunicação que promovam essas notificações, nos termos previstos no RGPD.

Palavras chave: notificações de violações de dados pessoais; RGPD; proteção de dados.

Abstract

Data breaches are security incidents which infringe the fundamental right to data protection (Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union). Data breaches require a comprehensive response.

Recognising this, the European Union (EU) has adopted a legal framework on personal data protection, which highlights the need for transparency and accountability. One of the main innovations of the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679) is the obligation for data controllers to notify data breaches to the supervisory authorities - and in some cases, to the data subjects concerned.

The GDPR contains rules regarding the deadline for these notifications, the competent supervisory authority, the cases in which data subjects need to be notified, the consequences of non-notification, etc. (Articles 33 and 34 of the GDPR). However, it does not regulate the internal and external processes for the detection, reporting and mitigation of adverse effects, even though a personal data breach must be notified to the supervisory authority within 72 hours after the controller becomes aware of it.

Therefore, this paper intends to contribute to the reflection on data breach notifications, defining general lines of action, good practices and communication chains which facilitate such notifications in accordance with the GDPR.

Keywords: data breach notification; GDPR; data protection.

Agradecimentos

Muito agradeço ao meu Orientador Professor Doutor Carlos Caleiro e Co-Orientadoras Professora Doutora Luísa Neto e Professora Doutora Filipa Calvão pelos sábios conselhos, opiniões críticas, pela generosidade e partilha intelectual.

Agradeço ao Professor Doutor Nuno Santos o seu exemplo de raciocínio lógico e por me lembrar que uma tese deve responder a um problema.

Cumpre ainda agradecer a disponibilidade da empresa Vitae Professionals, Lda. e dos seus colaboradores – em especial à Dra. Ana Marta Santos e à Dra. Luísa Moreira –, que muito contribuíram para o teste da proposta de procedimento de notificação de violações de dados apresentada neste estudo.

Tenho ainda de agradecer ao Guillaume Byk e aos demais colegas da Autoridade Europeia de Proteção de Dados por diariamente me fazerem acreditar que as problemáticas relacionadas com a proteção de dados merecem ser pensadas com profundidade e que existem soluções para os problemas.

Por último, mas não menos importante, este trabalho não teria sido possível sem o apoio incondicional, paciência e carinho do Jens, da minha família e amigos.

Disclaimer

Este trabalho resulta da visão pessoal da sua autora e não da posição institucional da Autoridade Europeia para a Proteção de Dados, na qual aquela trabalha.

Índice

Lista de quadros e figuras

Lista de siglas, acrónimos e abreviaturas

AEPD	Autoridade Europeia para a Proteção de Dados
AIPD	Avaliação de impacto sobre a proteção de dados
Art.	Artigo
CCI	Centro Comum de Investigação
CEPD	Comité Europeu para a Proteção de Dados
Cf.	Conferir
CNPD	Comissão Nacional de Proteção de Dados
CRP	Constituição da República Portuguesa
ENISA	Agência da União Europeia para a Segurança das Redes e da Informação
EPD	Encarregado de Proteção de Dados
et. al.	Et altere
Etc.	Et cetera
EUA	Estados Unidos da América
EUROJUST	Unidade Europeia de Cooperação Judiciária
EUROPOL	Agência da União Europeia para a Cooperação Policial
FAQ	*Frequently Asked Questions*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LPD	Lei de Proteção de Dados
OPC	Órgãos de Polícia Criminal
p./pp.	Página/páginas
PDCA	*Plan, Do, Check and Act*
PME	Pequena e média empresa
RGPD	Regulamento Geral de Proteção de Dados pessoais
SGSI	Sistemas de gestão da segurança da informação
SI	Segurança da Informação
SMS	*Short message service*
ss.	Seguintes
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias da Informação e da Comunicação
UE	União Europeia
Vol.	Volume
VPN	*Virtual Private Network*
Vs.	Versus

Introdução

A humanidade tem assistido a contínuas revoluções tecnológicas, designadamente no que respeita às Tecnologias da Informação e da Comunicação (doravante TIC), que influenciam o modo de interação da sociedade e carecem de novas formas de proteção, tanto práticas como jurídicas. Para as gerações nascidas neste milénio, o convívio e utilização das TIC passou de precoce a indispensável e a absoluta dependência destas tecnologias parece ser uma tendência evidente não apenas para a mais jovem geração[1], como para a sociedade em geral.

Por um lado, são claramente reconhecidas as vantagens das TIC, dado que o seu progresso tecnológico encurta distâncias, aumenta a velocidade das interações, reduz custos, potencia a produtividade, automatiza tarefas repetitivas, promove o acesso à informação, etc., facilitando a vida profissional e pessoal da nossa sociedade. Por outro lado, encontramos características que podem ser vistas dualmente como vantajosas e desvantajosas, tal como a ubiquidade da tecnologia e a rápida difusão da informação que esbatem os limites da esfera pública e privada. Ademais, a Internet e as redes sociais possibilitam alargar o número de destinatários da informação publicada, mas não necessariamente por ser pública[2]. Por último, as TIC comportam também riscos, quer seja pela falta de garantias de segurança e de fiabilidade, pela possibilidade de agir sob anonimato, quer por outras razões (operações de tratamento de dados em grande escala, etc.), as quais colocam em causa a confiança dos utilizadores e os seus direitos fundamentais.

Na verdade, os riscos hodiernos para a reserva da intimidade da vida privada diferem muito daqueles que justificaram o aparecimento do direito à proteção da reserva da vida privada e do direito à proteção de dados. Em especial, um dos fatores que contribuiu em grande medida para essa diferença resulta do aparecimento de um novo palco de atuação para os domínios público e privado: o ciberespaço[3]. Neste novo espaço observamos uma multiplicidade de novos modos de inter-relacionamento social, económico, político, etc., mas também novos desafios, riscos e ameaças. Todavia, cumpre frisar que os valores, regras e princípios de Direito vigentes no mundo físico têm a sua aplicação plena no mundo virtual. Assim, os direitos fundamentais como o direito à proteção de dados, à segurança e à educação não são incompatíveis com o ciberespaço, sendo inclusivamente reforçados pela maior abrangência da sua aplicação nesta nova arena.

No entanto, a crescente interação dos diversos agentes no ciberespaço e o aumento das ameaças que ensombram este novo palco exigem uma atitude consciente e pró-ativa, em nome da manutenção da

[1] FUENTE ANUNCIBAY, Raquel, «ICTs and Teenage Students. Problematic Usage or Dependence» in Procedia - Social and Behavioral Sciences, Volume 237, 21 February 2017, Pages 230-236.

[2] Veja-se o exemplo do Wikileaks. Cf. MACEDO NASCIMENTO, Ademir, Quem Vigia o Vigilante? Uma Análise da Ação Social Weberiana Sobre o **Wikileaks®** in *Revista Eletrônica de Gestão Organizacional.* 2015 Special Edition, Vol. 13, p. 412-417.

[3] Cf. FARINHO, Domingos, Intimidade da Vida Privada e Media no Ciberespaço, Almedina, 2006.

segurança do ambiente em linha[4] e da proteção dos dados dos seus utilizadores. Vaticina a sabedoria popular que «o seguro morreu de velho e o desconfiado ainda é vivo». Todavia, mesmo aqueles que tomam as devidas precauções não podem assegurar a total eliminação dos riscos. Existe sempre alguém com motivação e tempo para testar os limites de segurança de um sistema, colocando em crise os direitos fundamentais dos cidadãos afetados. Sem prejuízo de a prevenção ser essencial, mais eficiente e menos onerosa para os seres humanos, no que respeita à proteção de dados pessoais, na verdade, é impossível assegurar que não ocorrerão violações de dados pessoais.

Nesta perspetiva, gostaríamos de sublinhar que não perfilhamos a ideia de que o recurso às novas tecnologias implica necessariamente uma violação dos direitos fundamentais dos seus utilizadores, nem a devassa da sua vida privada. Entendemos que as novas tecnologias devem encontrar-se ao serviço da sociedade, devendo os seus utilizadores ter uma atitude consciente relativamente aos seus riscos. Nesse sentido, é premente a consciencialização societal para a proteção e projeção da dignidade humana – princípio basilar na Constituição da República Portuguesa[5] e em qualquer estado de direito – face à possível intromissão das modernas tecnologias na esfera privada de cada cidadão.

De acordo com os dados do Eurobarómetro para a cibersegurança[6], os cidadãos europeus utilizadores da Internet revelam que a violação de dados pessoais constitui a sua principal preocupação quando realizam transações em linha. Aliás, constata-se um aumento desta preocupação por parte dos cidadãos europeus em 2017 (45% dos inquiridos), relativamente aos dados resultantes dos Eurobarómetros de 2014 (43% dos inquiridos) e de 2013 (37 % dos inquiridos).

A maior parte dos incidentes que colocam em crise a confidencialidade, a disponibilidade e a integridade dos dados pessoais resultam de erros humanos, de falhas técnicas, de ataques informáticos, *malware*, erros e ciber-espionagem[7]. Apesar de reconhecermos que a escala e o impacto das violações de dados pessoais são naturalmente potenciados pela utilização de TIC, alertamos que estas violações não têm de ser informáticas, podendo ser apenas físicas. Neste enquadramento, cumpre referir que as violações de dados podem ocorrer através de meios eletrónicos, mas também de meios não

[4] Apesar da linguagem informática ser maioritariamente na língua inglesa, na realização deste trabalho tentámos adotar uma tradução em língua portuguesa, sempre que possível. Contudo, advertimos que as traduções foram realizadas pela própria autora, pelo que as citações serão também transcritas na sua língua original.

[5] Cf. artigo 1.º da Constituição da República Portuguesa, que confere primazia ao princípio da dignidade humana relativamente à própria ideia de Estado de direito democrático, iniciando o seu articulado e baseando toda a construção da lei fundamental em torno deste princípio.

[6] Cf. Eurobarometer Europeans' attitudes towards cyber security, September 2017, p. 6 e 7, disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171.

[7] KARYDA & MITROU, Breach Notification: Issues and Challenges for Security Management, in Tenth Mediterranean Conference on Information Systems (MCIS), Paphos, Cyprus, September 2016, disponível em: https://www.researchgate.net/profile/Maria_Karyda/publication/309414062_DATA_BREACH_NOTIFICATION_ISSUES_AND_CHALLENGES_FOR_SECURITY_MANAGEMENT/links/580f4b4608aef2ef97afc0b2/DATA-BREACH-NOTIFICATION-ISSUES-AND-CHALLENGES-FOR-SECURITY-MANAGEMENT.pdf - p.2: *Most data breaches are currently a result of external actors such as hackers. Other sources include malware, social attacks, misuse by employees, physical action, errors and cyber espionage.*

automatizados, como veremos *infra*. Contudo, na «sociedade digital»[8] em que vivemos, o peso da tecnologia assume um maior destaque e possibilita uma maior escala, dimensão e impacto das violações de dados. A título de exemplo, um acesso físico por alguém não autorizado ao registo manual de entradas nas urgências de um hospital constitui uma violação de dados pessoais.

Sabendo que o erro faz parte da condição humana, não podemos pretender viver num mundo utópico, sem erros, sem falhas, sem «calcanhares de Aquiles», mesmo que o desejemos. Por essa razão e com vista a melhor reforçar os direitos dos cidadãos – e, em especial, os direitos fundamentais –, é necessário conhecer os possíveis riscos decorrentes dos erros, mas também de outras fontes (por exemplo, falhas técnicas, ataques informáticos deliberados, etc.), e prepararmo-nos para os mesmos.

Com o propósito de colmatar as diferenças nas garantias à proteção de dados pessoais entre os diversos ordenamentos jurídicos da União Europeia (UE), o legislador europeu decidiu adotar em 2016 um regulamento geral – Regulamento Geral de Proteção de Dados pessoais (RGPD)[9] – para uniformizar o nível de proteção dos cidadãos nestas matérias. Entre as novidades deste regulamento encontramos a obrigatoriedade das notificações de violações de dados pessoais para todos os responsáveis pelo tratamento de dados, com a expectativa de permitir a tomada de medidas e precauções necessárias por parte das autoridades de controlo e dos próprios titulares dos dados potencial ou efetivamente afetados. Daqui resulta a maior responsabilização dos responsáveis pelo tratamento, mas também a maior transparência e capacitação dos titulares dos dados afetados.

No entanto, a obrigatoriedade legal destas notificações de violações de dados contém vários conceitos indeterminados e requer uma planificação prévia para que a celeridade desejável nesta cadeia de informação até aos titulares dos dados não seja comprometida. Pese embora o RGPD configure um avanço em matéria de proteção de dados e, em particular, no que respeita às violações de dados pessoais, a maior responsabilização dos responsáveis pelo tratamento de dados para a efetiva observância do seu texto é também patente. Desde logo, a obrigação que impende sobre os responsáveis pelo tratamento de notificarem a autoridade de controlo competente, bem como os titulares dos dados afetados, exige a sua maior intervenção – nomeadamente na adoção de medidas de segurança adequadas e de um plano eficiente de comunicações internas e externas. Após uma violação de dados pessoais, o tempo corre contra os potenciais lesados e cada minuto conta para uma reação adequada e atempada.

Face ao *supra* exposto, este trabalho pretende analisar a importância das notificações de violações de dados pessoais às autoridades de controlo e aos titulares dos dados afetados nos termos e para efeitos dos artigos 33.º e 34.º do RGPD. Nesse sentido, e para promover o cumprimento destas disposições legais, enunciaremos um conjunto de boas práticas relacionadas com a notificação de violações de

[8] Cf. VAN WEERT, Tom, K. MUNRO, Robert, Informatics and the Digital Society – Social, Ethical and Cognitive Issues, Springer, 2003.

[9] 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 (Regulamento Geral sobre a Proteção de Dados – RGPD).

dados pessoais, entre as quais propomos um procedimento para comunicações internas e externas que facilita a notificação atempada das violações de dados pessoais à autoridade de controlo. Por fim, demonstraremos a eficácia deste procedimento de comunicações através do seu teste numa empresa portuguesa.

Gostaríamos de sublinhar que este trabalho se destina a sensibilizar juristas, encarregados de proteção de dados, engenheiros informáticos, peritos na área das TIC, responsáveis pelo tratamento de dados para a importância das notificações de violações de dados pessoais e dos seus requisitos, nos termos do RGPD, assim como para a exequibilidade de um procedimento de notificações de violações de dados pessoais entre os diversos atores envolvidos num tratamento de dados, o qual facilitará o cumprimento das obrigações legais. Para tanto, procurámos adotar uma linguagem e terminologia inteligíveis a todos os destinatários, ainda que com uma acentuação técnico-jurídica por (de)formação profissional da sua autora.

Não tendo a pretensão de abarcar todas as problemáticas adjacentes à temática das violações de dados pessoais, esclareça-se finalmente, *ad limine, que* este estudo não versa sobre as notificações gerais de violações de dados pessoais ao abrigo de outra legislação específica, como é o caso da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). Encontra-se também fora do escopo deste trabalho a temática da cibersegurança, cibersegurança forense, as avaliações de impacto sobre a proteção de dados pessoais, a adequação das medidas de segurança da informação, gestão do risco, entre outras.

I. Violações de dados pessoais

As violações de proteção de dados podem ter vários níveis de complexidade e impacto, pelo que comportam várias perspetivas. No entanto, uma vez que este trabalho apenas versará sobre as notificações de violações de dados pessoais, este primeiro capítulo será dedicado às violações de proteção de dados numa perspetiva sumária e genérica, para enquadramento desta temática no âmbito deste estudo.

Nesse sentido, este capítulo será dedicado à análise de alguns conceitos-chave para a cabal compreensão das violações de dados pessoais, do direito à proteção de dados, do regime e das consequências jurídicas da recente alteração paradigmática da legislação em matéria de proteção de dados − incluindo a extensão da sua aplicação territorial −, seguindo-se uma descrição das tipologias de violações de dados, uma breve alusão à avaliação do risco e, por fim, a exemplificação de eventuais consequências e danos dali resultantes.

1. Conceitos-chave relativos à proteção de dados

Com vista à compreensão do objeto de estudo deste trabalho, comecemos pela definição de alguns conceitos basilares, nomeadamente de dados pessoais, de tratamento de dados, de titular dos dados, categorias especiais de dados e de violação de dados pessoais. Aliás, a definição de tais conceitos resulta hoje expressamente do RGPD, não obstante a clara crítica que se pode fazer a essa opção do ponto de vista das boas práticas da legística.

No n.º 1 do artigo 4.º do RGPD, define-se como «dados pessoais» a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»), sendo considerada uma pessoa singular identificável aquela 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 da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

No mesmo regulamento encontramos a seguinte definição de «tratamento»: operação ou conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição[10]. A Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados, doravante LPD) também contém uma definição muito próxima da *supra* definida no RGPD[11].

[10] Cf. n.º 2 do artigo 4.º do RGPD.

[11] De acordo com a alínea b) do artigo 3.º da LPD, entende-se por «tratamento de dados pessoais» qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a

Simultaneamente, a mesma lei distingue, dentro da classificação genérica de dados pessoais, uma categoria de dados à qual atribui uma proteção acrescida: os dados pessoais sensíveis[12] – segundo a terminologia da LPD (cf. artigo 7.º da LPD[13]) – ou categorias de dados especiais, de acordo com a designação do RGPD (cf. artigo 9.º do RGPD).

Segundo o n.º 1 do artigo 9.º do RGPD, consideram-se categorias especiais de dados pessoais aqueles que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados genéticos, biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde, bem como à orientação e vida sexual[14]. Nestas categorias especiais de dados incluem-se também os dados relativos a condenações penais e infrações (cf. artigo 10.º do RGPD), que devido à sua especial sensibilidade mereceram um articulado autónomo por parte do legislador – designadamente porque algumas das exceções à proibição do tratamento das categorias especiais de dados elencadas no artigo 9.º do RGPD não se aplicam às condenações penais e infrações previstas no artigo 10.º do mesmo diploma.

De acordo com o n.º 12 do artigo 4.º do RGPD, uma «violação de dados pessoais» consiste numa violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

2. Direito à proteção de dados – enquadramento jurídico

Comece-se inelutavelmente por fazer relevar a importância da temática da proteção de dados e, consequentemente, das notificações de violações de dados, bem como o reflexo das recentes alterações legislativas a este respeito. Atentemos, portanto, sobre o respetivo fundamento, *id est,* direito à proteção de dados pessoais que é um direito fundamental reconhecido no n.º 1 do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (doravante, a Carta)[15] e também no n.º 1 do artigo 16.º

organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição.

[12] A expressão «dados sensíveis» parece traduzir bem a especial natureza destes dados, os quais merecem uma proteção acrescida.

[13] Nos termos do n.º 1 do artigo 7.º da LPD, os dados pessoais são referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos.

[14] De notar que relativamente à definição de dados sensíveis constante da LPD, as categorias especiais de dados do RGPD não referem os dados da vida privada como dados merecedores per se de uma proteção acrescida. A este respeito, o legislador nacional foi mais exigente do que o legislador europeu. Embora haja um alinhamento entre as duas definições, não há uma sobreposição absoluta.

[15] Artigo 8.º (Proteção de dados pessoais) da Carta dos Direitos Fundamentais da União Europeia (2000/C 364/01).
1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

do Tratado sobre o Funcionamento da União Europeia (TFUE)[16]. A nível nacional, para além de decorrer da previsão de proteção da reserva da intimidade de vida privada que resulta do artigo 26.º da lei fundamental, este direito encontra-se especificamente previsto – e, note-se, desde a versão originária de 1976 – no artigo 35.º da Constituição da República Portuguesa (CRP), a qual reflete os princípios axiológicos basilares de uma determinada sociedade[17], bem como o seu estádio de evolução[18]. Assim, sendo constitucionalmente consagrado, o direito à proteção de dados adquire a designação de direito fundamental e é sempre expressão do princípio da dignidade da pessoa humana, fundamento último da CRP[19].

Contudo, apesar de se tratar de um direito fundamental, a efetiva fruição do direito à proteção de dados é uma conquista frágil nos nossos dias. Como já se salientou e retomaremos adiante, são vários os exemplos de violações deste direito fundamental. Não falamos aqui da habitual ponderação com outros direitos e interesses constitucionalmente protegidos, tal como sucede com os demais direitos fundamentais – dado o direito à proteção de dados pessoais não se tratar de um direito absoluto. Essa ponderação casuística − designadamente com o direito à segurança, o direito à identidade, etc. − é necessária para a aferição da proporcionalidade em situações de conflito e colisão de direitos com vista ao normal funcionamento de uma sociedade. Nas palavras de Jorge Miranda, «*somente há direitos fundamentais (…) quando o Estado e a pessoa, a autoridade e a liberdade se distinguem e até, em maior ou menor medida, se contrapõe*»[20], não sendo o direito à proteção de dados pessoais exceção a esta regra. Falamos, outrossim, de tentativas e efetivas violações do direito à proteção de dados pessoais sem qualquer justificação jurídica. Por essa razão, impõe-se uma maior visibilidade a este direito fundamental e à sua efetiva proteção e reforço, especialmente nos casos de violações do mesmo.

Debrucemo-nos, especificamente, sobre os referidos artigos 26.º e 35.º da CRP. Começando pelo primeiro, constatamos que o n.º 2 do artigo 26.º da CRP remete para a lei o estabelecimento de garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias. Um dos diplomas legais que materializa esta imposição

3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[16] Artigo 16.º do TFUE (ex-artigo 286.º TCE)
1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes.
As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39.º do Tratado da União Europeia.

[17] Aliás, o artigo 1.º da CRP ao reconhecer, em primeiro lugar, a dignidade humana como valor logicamente anterior à própria ideia de Estado de Direito democrático, atribui a acentuação tónica da sua construção ao ser humano. Por outras palavras, será no respeito pela dignidade da pessoa humana que o texto constitucional assentará.

[18] Sobre a evolução histórica do direito à reserva da vida privada, veja-se JIMÉNEZ, Luis, «Evolución histórica y conceptual del derecho a la vida privada», in *Revista de Los Tribunales Agrarios*, Segunda Época, n.º 42, año IV, Mayo-Agosto de 2007.

[19] Cf. Artigo 1.º da CRP.

[20] MIRANDA, Jorge, Manual de Direito Constitucional, 3.ª Edição, Coimbra Editora, 2000, Tomo IV, p. 12.

constitucional é a LPD, dispondo o seu artigo 2.º que o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais. O entendimento subjacente a este diploma espelha que a efetiva garantia contra a obtenção e utilização abusivas de informações relativas ao indivíduo e à família se traduz na observância dos princípios da finalidade, da legalidade, da necessidade, da adequação, da proporcionalidade em sentido estrito e da não discriminação, enquanto decorrência do princípio da igualdade.

No entanto, cumpre referir que o quadro legislativo do qual faz parte a LPD – e que resulta da transposição da Diretiva n.º 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 – sofreu recentemente uma profunda alteração. Assim, o 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 (Regulamento Geral sobre a Proteção de Dados - RGPD[21]) veio revogar aquela Diretiva e entrou plenamente em vigor no dia 25 de maio de 2018. Devido à sua pertinência, esta análise das violações de dados pessoais irá referir as disposições da LPD – ainda vigente, mas a ser brevemente revogada (proposta de lei do Governo em fase de preparação[22]) –, mas sobretudo do RGPD, também em vigor e imediatamente aplicável.

Sem prejuízo do *supra* exposto, sublinhe-se que o RGPD é uma evolução e não uma revolução do regime de proteção de dados pessoais. Não se trata de uma mudança drástica em relação ao regime anteriormente em vigor, mas antes uma mudança na abordagem à proteção de dados pessoais, na medida em que impõe mais medidas preventivas (por exemplo, a privacidade desde a conceção e por defeito – cf. artigo 25.º do RGPD), novas obrigações aos responsáveis pelo tratamento de dados (cf. artigo 35.º do RGPD – avaliação de impacto sobre a proteção de dados[23], artigo 33.º – notificação de uma violação de dados pessoais à autoridade de controlo, e n.º 5 do artigo 83.º – condições gerais para aplicação de coimas), assim como estabelece uma maior monitorização e controlo por parte dos titulares dos dados (cf. artigo 34.º do RGPD – comunicação de uma violação de dados pessoais ao titular dos dados).

Regressando à análise do artigo 26.º da CRP, verifica-se que o n.º 3 deste artigo vem sublinhar a defesa da dignidade humana, colocando algumas reservas quanto à utilização de tecnologias e à

[21] O RGPD – que resultou de um processo legislativo moroso e complexo – pretende, em primeira linha, simplificar o quadro regulatório em matéria de proteção de dados e devolver aos titulares dos dados o controlo sobre os seus dados pessoais. Este Regulamento foi publicado no Jornal Oficial da União Europeia a 4 de maio de 2016 e entrou em vigor em 24 de maio de 2016. Todavia, apenas é plenamente aplicável a partir de 25 de maio de 2018.

[22] Cf. a proposta de lei em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368.

[23] Cf. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, de 3 de outubro de 2017 e revistas em 4 de outubro de 2017: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

experimentação científica. Esta preocupação do legislador constitucional deve-se aos abusos cometidos no passado – designadamente durante a II Guerra Mundial – ao abrigo da ciência e de outros discursos legitimadores, assim como à incerteza e incompreensão do caminho a trilhar num século marcadamente caraterizado pela revolução tecnológica.

Passemos agora à análise do artigo 35.º da CRP[24]. Na mesma senda do artigo 26.º da CRP, e dele manifestamente decorrente, o artigo 35.º da CRP vem também debruçar-se sobre a utilização da informática[25], sempre com vista à defesa da dignidade humana[26].

O n.º 1 do artigo 35.º da CRP prevê os direitos de acesso, de retificação, de atualização, de informação, que são densificados nos artigos 12.º a 19.º do RGPD – o qual inclui também o direito ao apagamento e à limitação do tratamento (cf. artigos 17.º e 18.º do RGPD). Trata-se de direitos da maior importância, na medida em que permitem ao titular dos dados um controlo efetivo da informação que lhe respeita. Daqui se conclui que o direito à proteção de dados se manifesta tanto numa perspetiva negativa – o direito a não ser incomodado, a ser esquecido (cf. artigo 17.º do RGPD), o direito a não ser sujeito a uma decisão tomada exclusivamente com base no tratamento automatizado (cf. artigo 22.º do RGPD) –, como também numa perspetiva positiva – direito à informação (cf. artigos 13.º e 14.º do RGPD), ao acesso (cf. artigo 15.º do RGPD), à retificação (cf. artigo 16.º do RGPD), à notificação de violações de dados pessoais (cf. artigo 34.º do RGPD), etc[27].

---

[24] Artigo 35º (Utilização da Informática)

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

[25] Cumpre referir que a Constituição da República Portuguesa de 1976 foi a primeira a consagrar o direito à privacidade, na sua vertente de proteção dos dados pessoais informatizados, de entre o catálogo de direitos, liberdades e garantias. Cf. VARGES GOMES, Mário, Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência, Centroatlantico.pt, 2006, p. 27.

[26] A título de enquadramento jurídico, importa esclarecer que a lei a que os n.ºs 1, 2, 6 e 7 deste artigo se reportam é atualmente o RGPD, bem como a Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados – LPD) até ao momento da sua revisão em conformidade com este regulamento.

[27] Na verdade, o RGPD vem acentuar a tónica da responsabilização do responsável pelo tratamento, assim como a maior transparência no tratamento de dados pessoais para que o titular dos dados obtenha um maior controlo sobre os seus dados pessoais.

Ainda neste âmbito, cumpre ressaltar que é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei[28].

Não poderíamos terminar este primeiro subcapítulo sem referir que a proteção de dados pessoais tem um escopo maior do que a segurança da informação. Na verdade, a proteção de dados compreende a segurança da informação, mas não se limita a assegurar a confidencialidade, disponibilidade e integridade da informação. Como vimos, trata-se de um direito fundamental, ou seja, um direito consagrado na lei fundamental de uma determinada sociedade que reflete o conteúdo mínimo intrínseco e inalienável à condição e dignidade humanas[29].

A este propósito cumpre distinguir o direito à proteção de dados pessoais de um outro direito fundamental, o direito à segurança (cf. n.º 1 do artigo 27.º da CRP). Na verdade, estes dois direitos − como muitos outros direitos fundamentais − sobrepõem-se em certa medida. Podemos constatar esse facto no que respeita à segurança da informação. A este propósito, a segurança da informação enquadra-se no direito à segurança (cf. n.º1 do artigo 27.º da CRP[30]).

Ora, entende-se por Segurança da Informação (SI)[31] a capacidade de proteger e assegurar a confidencialidade, integridade e disponibilidade da informação detida por uma entidade pública ou privada [32]. De um modo resumido, a confidencialidade da informação pode ser obtida graças ao controlo de acessos, à cifragem dos dados, à aplicação de procedimentos de autorização, entre outras medidas. A integridade da informação assenta na validação de que o conteúdo da informação é transmitido exatamente como foi rececionado, garantindo a confiança no sistema de informação. Por último, a disponibilidade da informação permite que aqueles que têm permissão de acesso possam consultar os dados sempre que necessário.

A SI é, portanto, um dos pilares da sociedade, dos indivíduos e das organizações. Por um lado, porque protege os direitos subjetivos das próprias pessoas singulares e coletivas, a SI permite a existência das mesmas, a sua coexistência no ecossistema interno e externo e o seu desenvolvimento ou expansão, respondendo às suas necessidades dentro dos limites consagrados na lei. Por outro lado, a SI protege também os direitos dos cidadãos e entidades com quem as organizações interagem direta e

[28] A título de exemplo, veja-se os pressupostos jurídicos das escutas telefónicas (artigo 126.º do Código de Processo Penal) e das ações encobertas (cf. Lei n.º 101/2001, de 25 de agosto). De modo a garantir a sua constitucionalidade, as diligências processuais de recolha de prova que interfiram na privacidade do suspeito ou arguido sem o seu consentimento terão de ser excecionais, basear-se necessariamente numa previsão legal, em despacho judicial e na ponderação dos direitos e bens jurídicos em causa, na perspetiva da proporcionalidade e da subsidiariedade.

[29] Contudo, tal não significa que se trate de um direito absoluto, como vimos.

[30] Artigo 27.º da CRP (Direito à liberdade e à segurança):
1. Todos têm direito à liberdade e à segurança.

31 Cf. ANDRESS, Jason, The Basics of Information Security – Understanding the Fundamentals of InfoSec, in *Theory and Practice*, 2.ª edição, Elsevier/Syngress, 2014.

[32] Cf. BOYCE, Joseph, JENNINGS, Dan, Information Assurance – a practical guide: Managing Organizational IT securit risks, Butterworth Heinemann, 2002.

indiretamente (por exemplo, clientes, trabalhadores, subcontratados, etc.), aumentando a confiança dos primeiros nas segundas e, consequentemente, a credibilidade destas últimas junto da sociedade.

Aliás, a medição do sucesso de uma organização terá também de atender ao grau de proteção conferido aos seus direitos, assegurando nomeadamente que a tecnicidade dos seus produtos ou serviços possui um valor económico, cujo mercado esteja disposto a pagar (existência), mas também que a sua estrutura orgânica interna valorize cada um dos seus colaboradores ao mesmo tempo que promova um espírito de equipa focado em objetivos comuns (coexistência) e, por último, defenda uma cultura una, com caráter duradouro, assente em valores partilhados por todos e que atenda às necessidades dos clientes/utentes, procurando o desenvolvimento da própria organização (expansão). Deste modo, afigura-se fundamental para a continuidade de uma organização que esta procure não só o justo equilíbrio entre os três vetores acima enunciados, como também a resposta às necessidades do mercado, atendendo à sua área geopolítica.

Tais propósitos não se esgotam na previsão do direito à proteção de dados pessoais. Como vimos, o direito à proteção de dados é um direito fundamental inerente à dignidade humana, reconhecido às pessoas singulares e coletivas [33], o qual não se resume à mera segurança da integridade, confidencialidade e disponibilidade da informação. Assim, sem prejuízo de garantir a segurança da informação, o direito à proteção de dados pessoais salvaguardará outras questões mais profundas e inerentes à condição humana[34].

A propósito da segurança da informação, não poderíamos deixar de falar na cibersegurança, atendendo à «sociedade em rede»[35] em que vivemos.

Do ponto de vista regulamentar, a temática da cibersegurança motivou os seguintes textos jurídicos pertinentes quanto à proteção de dados pessoais:

- a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;

[33] No entanto, cumpre ressalvar que o objeto do RGPD é o estabelecimento de regras relativas às pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (cf. n.º 1 do artigo 1.º do RGPD). Todavia, encontramos exceções a esta regra, já que os dados pessoais não deixam de sê-lo mesmo quando sejam também dados de pessoas coletivas. Por exemplo, se o nome de uma pessoa coletiva incorpora o nome dos seus sócios (pessoas singulares), identificando-os, então estamos perante dados pessoais, merecedores da proteção conferida no corpus legislativo nesta matéria.

[34] É por esta razão que normas de certificação destinadas unicamente à segurança da informação, como por exemplo a International Standard ISO 27001, ficam aquém dos requisitos impostos pelo enquadramento jurídico da proteção de dados pessoais.

[35] CASTELLS, Manuel, A Era da Informação: Economia, Sociedade e Cultura, Volume I, A sociedade em rede, Fundação Calouste Gulbenkian, 2011.

- o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE;
- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) – ainda que presentemente em fase de revisão;
- Lei n.º 109/1009 de 15 de setembro, que aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa[36];
- o Decreto-Lei n.º 69/2014, de 9 de maio, que procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança.

No entanto, assinalam-se lacunas graves na regulação das temáticas da cibersegurança, desde logo relativamente à própria definição jurídica de ciberespaço – questão com a qual este trabalho de investigação não se vai deter, dado essa temática ser merecedora de uma análise em profundidade *per se*.

Ainda assim, a Comissão Europeia evidencia algumas preocupações na «Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido», constante da Comunicação Conjunta ao Parlamento Europeu ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões de 2013, sublinhando que «... a falta de acesso à Internet e a iliteracia digital constituem uma desvantagem para os cidadãos, tendo em conta a importância e a quase omnipresença do mundo digital nas atividades da sociedade»[37].

Por outro lado, indica ainda que «[t]odos os intervenientes relevantes, sejam as autoridades públicas, o setor privado ou os cidadãos individualmente, têm de reconhecer esta responsabilidade partilhada, tomar medidas para se protegerem e, se necessário, procurar uma resposta coordenada para reforçar a cibersegurança»[38].

Acresce que a Estratégia da União Europeia para a cibersegurança dedica um capítulo à sensibilização, no qual destaca que os «... utilizadores finais desempenham um papel crucial na garantia da segurança das redes e dos sistemas informáticos ...». Ademais, coloca em evidência o empenho da EUROPOL, EUROJUST, ENISA – *European Union Agency for Network and Information Security* e das autoridades

[36] VENÂNCIO, Pedro Dias, Lei do Cibercrime – Anotada e comentada, Coimbra: Coimbra Editora, 2011

[37] Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões de 2013 sobre a "Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido", p. 4.

[38] Cf. Ibidem, p. 8.

nacionais de proteção de dados na sensibilização dos utilizadores finais[39]. Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço[40] também denota a importância conferida à cibersegurança, considerando a segurança do ciberespaço uma das prioridades nacionais.

Partilhando igualmente esta preocupação com a cibersegurança, o RGPD vem reformular os princípios de proteção de dados, dando um enfoque particular ao princípio da responsabilidade. Na verdade, este princípio vem trazer uma nova tónica na divisão de responsabilidade. Por um lado, os responsáveis pelo tratamento têm de observar a legislação nesta matéria, bem como demonstrar o seu cumprimento. Por outro, os próprios titulares dos dados são chamados a intervir e a contribuir proactivamente para a sua autoproteção. Para tanto, exige-se uma maior transparência nos tratamentos de dados pessoais por parte dos responsáveis pelo tratamento.

Dediquemos agora a nossa atenção à análise da extensão da aplicação territorial do RGPD face ao anterior enquadramento jurídico.

3. A aplicação territorial do RGPD

O RGPD apresenta várias novidades e, em certa medida, altera o paradigma da proteção de dados pessoais. Entre as inovações incorporadas neste regulamento, encontramos o alargamento do âmbito territorial.

Lembremos que a legislação de proteção de dados não é idêntica em todo o mundo. A proteção imposta pela legislação da União Europeia é diferente das disposições vigentes nos EUA e noutras latitudes. Contudo, nos termos do artigo 3.º do RGPD, no que respeita ao âmbito de aplicação territorial, as disposições do RGPD aplicam-se aos tratamentos de dados pessoais:

- efetuados no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União Europeia (independentemente de esse tratamento ocorrer dentro ou fora da UE)[41]; ou
- cujos titulares se encontrem no território da UE, mesmo que o responsável pelo tratamento ou subcontratante não estejam estabelecidos na UE, quando as atividades de tratamento estejam relacionadas (a) com a oferta de bens ou serviços (independentemente de exigirem um pagamento)[42] ou (b) com o controlo do seu comportamento, o qual tenha lugar na UE[43];

[39] Cf. Resolução do Conselho de Ministros n.o 36/2015, publicada no Diário da República, 1.a série, n.º 113, de 12 de junho de 2015.

[40] Cf. Resolução do Conselho de Ministros n.º 36/2015, publicada no Diário da República, 1.ª série, n.º 113, de 12 de junho de 2015.

[41] Cf. N.º 1 do artigo 3.º do RGPD.

[42] Cf. Alínea a) do n.º 2 do artigo 3.º do RGPD.

[43] Cf. Alínea b) do n.º 2 do artigo 3.º do RGPD.

- realizados por um responsável com sede fora da UE, mas num país onde se aplique o direito de um Estado-Membro, por força do direito internacional público[44].

Este alargamento do âmbito territorial face à legislação anterior[45] vem subordinar os tratamentos de dados pessoais de cidadãos que se encontrem no território da UE[46] – independentemente da sua nacionalidade – efetuados por entidades estabelecidas em países terceiros (por exemplo, nos Estados Unidos da América, Rússia ou China) ao regime do RGPD.

Na verdade, a abrangência territorial do RGPD afigura-se particularmente relevante num mundo cada vez mais dependente das TIC e marcado por alguns «gigantes tecnológicos»[47] – como a Google, Facebook, Microsoft, etc. – com sedes fora da UE. Por isso, o âmbito de aplicação territorial do RGPD foi alargado relativamente ao quadro normativo anterior, com vista a garantir que o regime de proteção de dados pessoais dos cidadãos que se encontravam na UE não fosse diminuído por via da aplicação da legislação da sede dos responsáveis pelo tratamento e dos subcontratantes. Esta opção legislativa teve em consideração a atual realidade das TIC. Estando a UE numa posição dianteira em matéria de proteção de dados a nível mundial, mas encontrando-se muitos dos responsáveis pelo tratamento ou subcontratantes – em especial na área das TIC – fora do espaço económico europeu, o regime do RGPD seria ineficaz se o âmbito de aplicação territorial se limitasse à territorialidade das suas sedes[48].

Por outro lado, não deixa de ser curioso que os responsáveis pelo tratamento e subcontratantes sedeados em países onde a legislação de proteção de dados pessoais oferece menos garantias do que a legislação europeia, tenham de aplicar o RGPD relativamente aos cidadãos que se encontrem na UE. Deste modo, na prática, os cidadãos de países cujas legislações possuam menor exigências relativamente à proteção de dados (independentemente da sua nacionalidade) encontram-se

---

[44] Cf. n.º 2 do artigo 3.º do RGPD.

[45] Cf. Diretiva n.º 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.

[46] Cf. Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados publicada no Jornal Oficial da União Europeia de 23.05.2018, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679R(02)&from=EN. O texto inicial referia-se aos «cidadãos residentes no território da UE», pelo que a atual redação alarga ainda mais o âmbito de aplicação do RGPD.

[47] Os «gigantes tecnológicos», quer pelo seu valor em bolsa, quer pela sua abrangência populacional (tanto em número como em representatividade à escala mundial), quer pela sua vasta recolha de informação têm uma presença notória na nossa sociedade. Cf. GALLOWAY, Scott, The four: the hidden DNA of Amazon, Apple, Facebook and Google, Random House Large Print, 2017.

[48] Aliás, algumas empresas norte-americanas preferiram deixar de operar tratamentos de dados pessoais no território da UE, pois entenderam ser mais penalizador cumprir com os requisitos impostos pelo RGPD do que perder a clientela europeia. Cf. HERN, Alex, WATERSON, Jim, "Sites block users, shut down activities and flood inboxes as GDPR rules loom", in The Guardian, 24.05.2018, disponível em: https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect. Destacamos «…*Instapaper, a service owned by the US firm Pinterest which enables users to save articles to read at a later date, became the latest to disconnect European customers on Thursday*…».

protegidos na UE por um regime jurídico mais garantístico do que quando se encontrem no seu país de origem.

Feito este enquadramento jurídico da aplicação territorial do RGPD, passemos à descrição das diferentes tipologias de violações de dados pessoais.

4. Tipologias de violações de dados pessoais

As violações de dados estão intimamente relacionadas com a segurança da informação, pelo que intrinsecamente associadas a incidentes que comprometam a confidencialidade, a integridade e/ou a disponibilidade dos dados pessoais.

Todavia, a proteção de dados pessoais tem um alcance diferente da mera segurança da informação, como vimos. Por essa razão, há incidentes relativos à segurança da informação que não comportam violações de dados pessoais. Tomemos como exemplo deste cenário um acesso não autorizado, por um hacker, a dados estatísticos ou fictícios num projeto em fase de teste, o qual não continha qualquer informação pessoal de indivíduos. Trata-se de uma falha de segurança da informação, mas não uma violação de dados pessoais.

Já o inverso não se aplica, dado que uma violação de dados pessoais implica, via de regra, um incidente de segurança. Nessa medida, podemos subsumir as violações de dados pessoais em três categorias relativas ao comprometimento da:

- confidencialidade;
- integridade; e
- disponibilidade.

Portanto, vejamos as diferenças entre cada uma das violações de dados pessoais acima elencadas. Uma violação de dados que comprometa a confidencialidade significa que alguém, acidentalmente ou sem autorização, divulgou ou acedeu a determinados dados pessoais. Diferentemente, numa violação que coloque em causa a integridade dos dados, não estará apenas em causa a divulgação não autorizada ou acidental dessa informação, mas também a sua alteração. Já no que concerne a uma violação de dados relativa à disponibilidade dos mesmos, estamos perante uma perda, destruição ou obstrução do acesso à informação pessoal.

Estas diferentes tipologias de violações de dados podem ocorrer separada ou simultaneamente, sendo possível que uma violação de dados pessoais comprometa os três elementos da segurança da informação *supra* vistos, ou que apenas contenda com um deles. De notar ainda que as violações de dados podem respeitar à totalidade dos dados pessoais de um sistema ou apenas aos dados de um único indivíduo. De outra banda, estas violações podem ser temporárias (como por exemplo, uma falha de acesso durante duas horas) ou definitivas (exemplificativamente, se uma empresa não efetuar back-

ups e um hacker efetuar um ataque aos seus servidores e eliminar a informação constante dos mesmos).

Acresce que estas violações de dados podem advir tanto internamente de uma entidade, como serem fruto de uma ação externa à mesma. Por exemplo, se um funcionário de uma empresa de análises clínicas inadvertidamente enviar um email com os resultados das análises de algumas pessoas para destinatários errados, está a cometer uma violação de dados pessoais comprometendo a confidencialidade dos mesmos, tendo a violação sido cometida a partir da própria entidade. De outro modo, se um *hacker* informático lançar um ataque de *ransomware*[49] aos servidores de um hospital, estamos perante um ataque externo que pode comprometer não só a confidencialidade, mas também a integridade e disponibilidade dos dados, caso não haja *backups* da informação.

O governo inglês publicou em abril de 2018 um estudo sobre violações de cibersegurança nas empresas e instituições de caridade[50] no qual revelou a natureza e impacto de ciber ataques no Reino Unido. Pese embora este estudo se circunscreva a organizações do Reino Unido, podemos retirar conclusões interessantes sobre as principais ameaças e o impacto das violações de dados no ciberespaço. Em primeiro lugar, destaca-se o facto de a grande maioria das empresas e instituições de caridade inglesas, independentemente do seu tamanho, recorrerem a serviços online, expondo-se assim a riscos de cibersegurança.

Em segundo lugar, sublinha-se que uma maioria significativa das grandes empresas (72%) e instituições de caridade (73%) inglesas foram alvo de incidentes de segurança ou ciberataques em 2017. De entre os ataques mais comuns, a receção de emails fraudulentos lidera a lista, seguida pela usurpação de identidade em emails ou websites, vírus/*spyware*/*malware* e *ransomware*.

Por último, pese embora este estudo tenha sido realizado um mês antes da entrada em vigor do RGPD – o qual é plenamente aplicável no Reino Unido – apenas 38% das empresas da amostra do estudo estava ciente deste regulamento e desse número apenas 13% alteraram as suas políticas de cibersegurança em conformidade com o regulamento.

Terminada esta análise das tipologias de violações de dados pessoais, atentemos agora na avaliação e gestão do risco, um dos aspetos mais caros às violações de dados pessoais.

---

[49] De acordo com a definição da empresa de antivirus AVG, entende-se por «*ransomware: malicious software which encrypts files on your computer or completely locks you out. It's spread by hackers who then demand a ransom (usually 300-500$/GPB/EUR, preferably paid in bitcoins), claiming that, if you pay, you'll receive the decryption key to recover your files».* Cf. https://www.avg.com/en/signal/what-is-ransomware.

[50] Cf. Cyber Security Breaches Survey 2018: Main report, Department for Digital, Culture, Media and Sport, disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

5. Avaliação e gestão do risco (Norma ISO 31000:2009)

O RGPD apresenta como nota distintiva face à Diretiva 95/46/CE um maior protagonismo da avaliação do risco. Contudo, pese embora este regulamento contemple várias referências aos riscos e ao impacto de violações de dados pessoais, não existe uma orientação concreta relativamente ao modo como deve ser aferido o risco.

Ora, para avaliar corretamente o risco, o responsável pelo tratamento terá de atender à tipologia da violação de dados, à probabilidade e gravidade dos efeitos negativos para os titulares dos dados, assim como à natureza, sensibilidade e volume dos dados pessoais em causa. Não podemos deixar de referir que a sensibilidade dos dados pessoais potencialmente afetados com uma violação de dados será um dos fatores mais relevantes.

Assim, na ausência de um apoio específico no RGPD para a aferição do risco, temos de socorrer-nos de outros instrumentos complementares. Entre estes, destacamos a norma ISO 31000:2009 – *Risk management – principles and guidelines* consiste num instrumento da *International Organization for Standardization* para a gestão do risco – pese embora não verse especialmente sobre a proteção de dados pessoais –, tendo por objetivo uniformizar a terminologia e conceitos que lhe são inerentes, assim como estabelecer os princípios e orientações para a implementação de um processo de análise, avaliação e gestão do risco, com vista a melhorar o desempenho das organizações nesta matéria.

Esta norma está estruturada em 4 etapas, conhecidas como o ciclo PDCA (*Plan, Do, Check and Act*). Deste modo, em primeiro lugar, tem de ser desenhado o enquadramento da gestão do risco (*plan*). Seguidamente, destaca-se a fase de implementação (*do*). A terceira fase respeita à monitorização e à análise (*check*), terminando a quarta e última fase com a melhoria contínua dos processos (*act*). Deste modo, as organizações não só têm uma perspetiva geral dos riscos que as podem afetar, como também conseguem que a gestão do risco responda às alterações que surjam posteriormente à sua implementação inicial.

Para compreender cabalmente a Norma ISO 31000:2009 importa perceber a sua definição de risco, como o «efeito (positivo ou negativo) da incerteza nos objetivos de uma organização»[51], sendo o risco expresso através da combinação das consequências de um determinado evento e a probabilidade associada à sua ocorrência. Nesta definição, a incerteza é entendida como o estado deficitário de informação – ainda que parcialmente – relacionado com a compreensão de um evento, com as suas consequências ou probabilidade de ocorrência. Daqui resulta uma perspetiva neutra do risco, já que pode ser positivo ou negativo, e as suas consequências podem potenciar ou diminuir os objetivos da organização.

A gestão do risco é facilitada pela sua associação em grupos consoante a relevância para a atividade da organização – por exemplo, riscos financeiros, riscos relativos à segurança da informação, etc.

[51] Cláusula 2.1 da norma ISO/IEC 31000:2009.

Feito este enquadramento, constatamos que o processo de gestão do risco na norma ISO 31000:2009 se inicia com a **A) contextualização do risco**, com base nos ativos da organização, ou seja, nos recursos que têm valor institucional e que devem ser protegidos ante as perdas ou prejuízos causados («*plan*» do ciclo PDCA).

De seguida, é fundamental a **B) avaliação do risco** *latu sensu*. Com esse intuito, é fundamental a identificação, análise e avaliação dos riscos. Para a identificação dos riscos, importa reconhecer:

- as **ameaças** – i.e., elencar os eventos não desejados que possam ocorrer, como ações maliciosas, catástrofes naturais, falhas de *hardware* ou de *software*;
- as **vulnerabilidades** – vistas como as fragilidades num ativo ou atividade que possam ser exploradas por uma ameaça para provocar perda ou dano, tendo consequentemente impacto na organização;
- a **probabilidade da sua ocorrência**; e
- o **controlo**, ou seja, quais os meios de proteção que permitem reduzir a vulnerabilidade de um sistema.

Já para a análise dos riscos terá de ser envidado um processo para compreender a natureza dos riscos eventuais e determinar o seu grau de gravidade. Esta aferição é relevante para estabelecer a posterior hierarquização de prioridades no seu tratamento, assim como para a alocação dos recursos financeiros e humanos necessários.

Na fase da avaliação do risco terá de se atender ao processo de comparação dos resultados da análise e dos critérios do risco para determinar se o mesmo e/ou a respetiva magnitude é aceitável ou não[52].

Feita esta avaliação do risco, segue-se a **C) gestão de riscos**, processo através do qual se identificam, controlam, minimizam ou eliminam os riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável («*do*» do ciclo PDCA). É nesta fase que se estabelecem as prioridades no tratamento dos riscos, os critérios de decisão, os prazos, o orçamento e os recursos necessários. Por conseguinte, é também neste momento que se atribuem as responsabilidades para cada risco e se definem os procedimentos de atuação. As estratégias para tratar os riscos podem implicar a sua mitigação através de controlos de segurança de informação e cibersegurança, a transferência do risco para terceiros (por exemplo para companhias de seguros) e o evitamento dos mesmos, prevenindo a causa ou os efeitos dos riscos.

Contextualizados e analisados os riscos, bem como implementada a sua gestão, segue-se a fase de **D) monitorização e aferição da eficácia da estratégia** anteriormente adotada («*check*» do ciclo PDCA). Este controlo através de auditorias periódicas e com critérios de medição objetivos permitirá reduzir os riscos e avaliar a eficácia das medidas de segurança adotadas que devem proteger

[52] Cf. «Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, the need for treatment can be considered.», ISO/IEC 31000:2009, p. 18.

eficazmente a organização contra as ameaças numa ponderação efetiva de custo-benefício. A reflexão daí resultante deverá ser comunicada aos órgãos dirigentes da organização e deverão ser atualizados os processos e procedimentos que careçam de melhorias («*Act*» do ciclo PDCA). É graças a este ciclo, o qual deve ser implementado continuamente, que a organização apresenta um percurso no sentido da melhoria contínua da sua gestão de riscos.

Ora, como *supra* visto, a identificação dos riscos de uma organização é fundamental para um processo efetivo da gestão dos mesmos. Uma vez que o risco resulta do binómio ameaça-vulnerabilidade, têm de ser chamadas à colação as possíveis combinações de ameaças e de vulnerabilidades que afetam ou podem afetar os ativos (incluindo os dados pessoais) ou a atividade da organização. Com essa finalidade, devem ser estimados os riscos através de uma forma de cálculo que associe a probabilidade da ocorrência das ameaças (fator ativo do risco) e o impacto associado à vulnerabilidade dos riscos (fator passivo).

Do ponto de vista qualitativo, o binómio probabilidade-impacto deve ser medido gradualmente em sentido crescente, tendo presente no eixo da probabilidade da sua ocorrência os eventos raros, pouco prováveis, de ocorrência moderada, prováveis e quase certos, e no eixo da gravidade do impacto os riscos insignificantes, *minor*, moderados, *major* e catastróficos. Aqui, o nível do risco (reduzido, moderado ou elevado) é estabelecido na interseção da escala da probabilidade e do impacto. Nesta perspetiva, é fundamental a hierarquização da probabilidade dos eventos e a avaliação qualitativa do seu impacto.

Do ponto de vista quantitativo, podem ser atribuídos valores ao fator probabilidade e ao fator impacto, da soma dos quais resulta um número que terá de ser confrontado com uma tabela previamente definida. Nessa tabela, constará uma escala com os valores de risco reduzido, médio e elevado. Concretizando esta ideia, tomando como referência uma escala na qual os valores até 3 são entendidos como riscos reduzidos, entre 4 e 7 vistos como riscos médios, e iguais ou superiores a 8, como riscos elevados, se ao risco x for atribuída a cotação 2 para a probabilidade e 5 para o impacto, conclui-se da soma com o valor final de 7 que o risco é médio.

Por último, sem prejuízo de existirem outras formas e escalas de aferição do risco, entendemos que a norma ISO 31000:2009 aborda os principais aspetos da avaliação e gestão do risco de um modo sistematizado, razão pela qual esta norma foi referida neste estudo.

Ante a necessidade de densificar alguns conceitos, o Grupo de trabalho do Artigo 29.º / Comité Europeu para a Proteção de Dados tentou elencar uma lista não exaustiva de exemplos de violações suscetíveis de implicar um risco elevado para os titulares dos dados[53]. O Comité Europeu para a Proteção de Dados (doravante CEPD) é um organismo europeu independente que tem como missão contribuir para a aplicação das regras em matéria de proteção de dados de um modo coerente na União Europeia,

[53] Cf. *Guidelines on Personal data breach notification under Regulation 2016/679*, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827, p. 31 e ss.

assim como promover a cooperação entre as diversas autoridades de proteção de dados nos 28 Estados-Membros da UE.

Este organismo foi estabelecido pelo RGPD e é composto por representantes das autoridades nacionais de controlo de proteção de dados e a Autoridade Europeia para a Proteção de Dados (AEPD). Na verdade, a diretiva 95/46/CE, que foi revogada pelo RGPD como já referido, já previa no seu artigo 29.º um grupo com caráter consultivo e independente de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, o qual foi literalmente apelidado de Grupo de Trabalho do Artigo 29.º Com o RGPD, este grupo de trabalho ganhou uma nova designação, um novo estatuto, bem como viu os seus poderes e missão ampliados.

Nesse sentido, o CEPD baseou a sua análise da suscetibilidade de um risco elevado para os direitos e liberdades quando a violação de dados pessoais possa originar danos físicos, materiais ou imateriais para os titulares dos dados[54].

Tendo presente esta ideia, a probabilidade e a gravidade dos riscos têm de ser tidas em conta aquando da aferição objetiva da suscetibilidade de a violação de dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares. Sublinhe-se, uma vez mais, que esta avaliação do risco difere da avaliação de impacto sobre a proteção de dados – AIPD (cf. artigo 35.º do RGPD), na medida em que se trata de uma avaliação concreta do risco e não hipotética. Tal significa que poderão existir riscos contemplados na AIPD que não se verifiquem numa determinada violação de dados em concreto, bem como riscos que não foram acautelados nessa previsão e que se verifiquem na prática[55].

Nos termos do considerando 75 do RGPD, a discriminação, a usurpação ou roubo de identidade, as perdas financeiras, os prejuízos para a reputação, as perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, a inversão não autorizada da pseudonimização ou quaisquer outros prejuízos importantes de natureza económica ou social são alguns dos exemplos que concretizam o risco para os direitos e liberdades das pessoas singulares. Adicionalmente, o considerando 85 do RGPD acrescenta a este elenco a perda de controlo sobre os seus dados pessoais e a limitação dos seus direitos.

Acresce que a Agência da União Europeia para a Segurança das Redes e da Informação (doravante ENISA) publicou em 2013 recomendações para uma metodologia da avaliação da gravidade de violações de dados pessoais (*Recommendations for a methodology of the assessment of severity of personal data breaches*[56]). De acordo com este documento, o contexto do tratamento de dados, a

[54] Idem, p.21.

[55] A este respeito e sem prejuízo da análise do caso concreto da violação de dados, refira-se que a AIPD deverá ser o mais abrangente possível e, portanto, idealmente deverá cobrir todos os riscos possíveis num determinado tratamento de dados pessoais.

[56] Cf. ENISA *Recommendations for a methodology of the assessment of severity of personal data breaches,* 2013, disponíveis em: https://www.enisa.europa.eu/publications/dbn-severity.

facilidade na identificação dos titulares dos dados e as circunstâncias da violação de dados pessoais devem ser tidas em consideração como critérios para avaliação da gravidade do risco.

No que concerne ao contexto do tratamento de dados, a ENISA elenca como fatores agravantes as características do responsável pelo tratamento (por exemplo, um hospital, uma farmácia, o Ministério da Segurança Social, etc.), o volume de dados pessoais (de um mesmo indivíduo) e a natureza dos dados (nomeadamente categorias especiais de dados pessoais) em causa na violação de dados pessoais, pois têm impacto na avaliação da gravidade do risco.[57]

O Grupo de trabalho do Artigo 29.º / Comité Europeu para a Proteção de Dados alerta para a tomada de consideração de violações de dados pessoais que envolvam categorias especiais de dados[58], ou titulares de dados vulneráveis (como crianças ou pessoas idosas).

A avaliação do risco será importante para a definição das medidas de segurança adequadas a um tratamento de dados, assim como para a resposta a uma violação de dados pessoais.

Veremos no ponto seguinte quais as possíveis consequências e danos resultantes de violações de dados pessoais.

6. Consequências e danos

Vimos no subcapítulo anterior alguns exemplos de riscos, como a discriminação, a usurpação ou roubo de identidade, etc.

Ora, através destes exemplos constatamos que as violações de dados pessoais podem resultar em danos patrimoniais, não patrimoniais, danos emergentes e lucros cessantes[59] para os titulares dos dados[60]. Ademais, segundo o estudo sobre violações de cibersegurança nas empresas e instituições de caridade *supra* mencionado[61], 37% dos ciberataques que as empresas inglesas sofreram em 2017 implicaram perdas financeiras e de dados. Contudo, apenas 2% das empresas e 1% das instituições de caridades afirmou que os dados pessoais que tratavam foram alterados, destruídos ou acedidos por pessoas não autorizadas. Ainda assim, sublinhe-se que alguns incidentes de segurança podem ter impacto nas organizações, mesmo quando não envolvam consequências financeiras ou a perda de

[57] Idem, p. 11.

[58] Como *supra* visto e definido, no capítulo I. Violações de dados pessoais. 1) Definição de conceitos-chave relativos à proteção de dados deste estudo.

[59] Segundo Jorge Ribeiro de Faria, o dano é «toda a perda causada em bens jurídicos, legalmente tutelados, de caráter patrimonial ou não(…) é o prejuízo que alguém sofre nos seus bens jurídicos por força de um comportamento ou acontecimento». Cf. RIBEIRO DE FARIA, Jorge, Direito das Obrigações – Volume I, Almedina, 2003, p.480 e 481.

[60] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827, p.21.

[61] Cf. Cyber Security Breaches Survey 2018: Main report, Department for Digital, Culture, Media and Sport, disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf.

dados pessoais. A falta de confiança dos clientes e utilizadores nas empresas e instituições pode colocar a atividade destas pessoas coletivas em risco[62].

Naturalmente que não descuramos que cada pessoa tem uma perceção muito própria da sua vida privada, o que também terá um reflexo no impacto das violações de dados pessoais. Os comportamentos dos cidadãos no mundo virtual e no mundo não digital são, de facto, bastante diferentes. Na verdade, por um lado, são inúmeros os exemplos de pessoas que não se inibem de partilhar aspetos íntimos da sua vida privada quando falam alto ao telemóvel em espaços públicos, ou quando partilham fotografias que revelam pormenores da sua esfera pessoal e familiar nas redes sociais on-line. Por outro, encontramos na nossa sociedade cidadãos preocupados com a proteção da sua vida privada, os quais não revelam ou procuram não revelar informações sobre a sua esfera privada e íntima.

Ainda que a definição da intimidade da vida privada seja delineada por cada indivíduo, alguns autores perfilham uma divisão dentro da intimidade da vida privada em três graus: uma esfera íntima, privada e social[63]. De todo o modo, os danos decorrentes de violações de dados pessoais podem afetar os seus titulares e causar-lhes prejuízos irreparáveis[64].

No entanto, mesmo nos casos em que haja um maior grau da exposição de dados pessoais pelos próprios titulares dos dados em determinados momentos, não se pode presumir o seu consentimento implícito para a divulgação dos seus dados pessoais a terceiros. Reitere-se que o direito à proteção de dados pessoais é um direito fundamental e, como tal, intrínseco à dignidade da pessoa humana. O direito à proteção de dados não tem como escopo a proteção dos dados *per se*, mas das pessoas aos quais os mesmos respeitam. Por essa razão, o direito à proteção de dados está umbilicalmente relacionado com a proteção da liberdade, e, em especial, da não discriminação, da liberdade de expressão, da igualdade, da imagem e da identidade, entre outros direitos fundamentais.

Ademais, as coimas e multas, os processos judiciais com possibilidade de penas efetivas, os danos reputacionais – quer para a organização (com a consequente perda de clientes, de lucro, de valor da marca, perda da vantagem competitiva, e a necessidade de aumentar custos com investimento em adotar uma nova estratégia de segurança/proteção de dados), quer para os colaboradores da organização (com impacto na sua carreira, com a possível perda do seu trabalho) – podem ser bastante

[62] De notar que o RGPD apresenta como novidade a necessidade de responsável pelo tratamento prever os riscos para si próprio, mas também para os titulares dos dados pessoais.

[63] Sobre o direito à reserva da intimidade da vida privada, e com particular enfoque no ciberespaço e perfilhando esta divisão tripartida, cf. FARINHO, Domingos Soares, Intimidade da Vida Privada e Media no Ciberespaço, Almedina, 2006, p. 43 e ss.

[64] Como exemplo, veja-se o caso da violação de dados pessoais da empresa Uber, o qual expôs nomes, números de telefone, endereços de email, número do cartão de crédito e informação sobre a geolocalização de mais de 57 milhões de utilizadores. Cf. CARRIE WONG, Julia, "*Uber concealed massive hack that exposed data of 57m users and drivers*", in The Guardian 22.11.2017, disponível em https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

superiores aos custos com medidas preventivas de violações de dados pessoais[65]. Apesar de estas violações não serem uma «pena de morte» para as empresas, não se ignoram os custos que lhes estão associados[66] [67].

Não menos importantes são os danos para os próprios titulares dos dados afetados. Na verdade, os danos causados por violações de dados pessoais, dependendo da sua natureza e impacto, podem ser muito marcantes para os titulares dos dados. As violações de dados pessoais podem resultar na usurpação de identidade ou noutras violações do direito à proteção de dados com impacto direto nos direitos fundamentais dos titulares, com eventuais prejuízos patrimoniais e não patrimoniais[68].

De outra banda, o reporte público da deteção de uma violação de dados pessoais, a reação adequada e célere, assim como a transparência de todo o processo através de uma estratégia de comunicação apropriada podem ser vistos como fatores que geram confiança e demonstram o cumprimento com as disposições legais em vigor, fomentando a imagem e a confiança no responsável pelo tratamento. Neste enquadramento, os titulares dos dados podem tomar medidas que tentem mitigar os potenciais danos decorrentes da violação.

Cumpre sublinhar que os benefícios de oficialmente informar as autoridades de controlo e, nos casos aplicáveis, também os titulares dos dados afetados, dando-lhes poder para atuar são comprovadamente superiores aos prejuízos associados à não comunicação atempada[69], quer relativamente às coimas aplicadas pela autoridade de controlo competente, quer aos danos reputacionais.

---

[65] Cf. The impact of data breaches on reputation & share value – a study of Marketers, IT Practicioners and Consumers in the United Kingdom, Ponemon Institute LLC patrocinado por Centrify, maio 2017, disponível em: https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf.

[66] Cf. LIEBER, Ron, How to protect yourself after the Equifax Breach, in The New York Times, 2017 (atualizado em 16.10.2017), disponível em: https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

[67] A empresa Über é um exemplo de recuperação de uma violação de dados pessoais. Pese embora tenha tentado ocultar essa violação de dados, continua atualmente a operar no mercado, o que demonstra que os seus utilizadores continuaram a confiar nesta empresa.

[68] A título de exemplo, veja-se a situação em que as coordenadas bancárias e os dados pessoais e um cidadão honesto são acedidos e utilizados por um *hacker*, que recorre a essa informação para efetuar compras on-line, esgotando o crédito desse cidadão. Se a perda de património não permitir que o cidadão honesto honre os seus compromissos financeiros, este perderá o seu bom nome junto da banca e ficará associado ao incumprimento.

[69] KELLY, Martin et al., Data Privacy: Effects on Customer and Firm Performance in Journal of Marketing, Sage Journals, Volume: 81 issue: 1, page(s): 36-58 October 8, 2018, disponível em http://journals.sagepub.com/doi/10.1509/jm.15.0497.

II. Notificações de violações de dados pessoais

Como visto *supra*, os artigos 33.º e 34.° do RGPD definem uma das principais novidades deste diploma legal: a obrigação de os responsáveis pelo tratamento de dados notificarem a autoridade de controlo competente e, em determinados casos, o próprio titular dos dados afetado, quando haja uma violação de dados pessoais. Veremos neste capítulo o objetivo destas notificações, quais as suas condições e procedimentos.

Preliminarmente, cumpre dizer que esta obrigação é um reflexo dos princípios da lealdade e transparência[70], da integridade e confidencialidade[71], bem como da responsabilidade[72] − presentes transversalmente no espírito do legislador europeu aquando da elaboração do RGPD. Nesse sentido, impende sobre o responsável pelo tratamento o ónus de reportar as violações de dados de que tiver sido alvo às autoridades de controlo com competência em matéria de proteção de dados pessoais e aos titulares dos dados, nos termos dos artigos 33.º e 34.º do RGPD.

De facto, estas notificações destinam-se a minimizar o impacto decorrente da violação de dados pessoais e a permitir uma resposta, quer por parte das autoridades de controlo, quer dos próprios cidadãos afetados. Precisamente porque estas notificações devem ocorrer rapidamente após a tomada de conhecimento por parte dos responsáveis pelo tratamento, como veremos em detalhe mais adiante, as organizações devem determinar previamente quais as entidades ou pessoas, a quem as violações de dados pessoais devem ser comunicadas e quais as informações a prestar. Sublinhe-se que nem todas as violações de dados têm de ser comunicadas às autoridades de controlo, nem aos titulares dos dados afetados, como melhor iremos analisar *infra*. Nesse sentido, importa compreender qual a informação necessária e relevante que deve ser comunicada, quais os destinatários e em que circunstâncias.

A este respeito, importa também referir que este dever de comunicar as violações de dados às autoridades de controlo competentes não é totalmente original. Na verdade, a Diretiva 2009/136/CE[73] e o Regulamento (EU) 611/2013[74] relativos às comunicações eletrónicas já haviam consagrado essa obrigação. No entanto, a inovação do RGPD consiste no alargamento da obrigação de violações de

[70] Cf. alínea a) do n.º 1 do artigo 5.º do RGPD.

[71] Cf. alínea f) do n.º 1 do artigo 5.º do RGPD.

[72] Cf. n.º 2 do artigo 5.º do RGPD.

[73] Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009 que altera a Diretiva/2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor, disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32009L0136&from=PT.

[74] Regulamento (EU) 611/2013 da Comissão, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas.

dados pessoais a todos os responsáveis pelo tratamento, e não apenas aos operadores de serviços de comunicações eletrónicas publicamente disponíveis[75].

Vejamos agora os termos e condições do RGPD relativamente às notificações de violações de dados pessoais às autoridades de controlo competentes, bem como as diferenças entre estas e as notificações aos titulares dos dados por elas afetados. Comecemos, então, por analisar o primeiro caso.

1. Notificação às autoridades de controlo

De acordo com o disposto no n.° 1 do artigo 33.° do RGPD, os responsáveis pelo tratamento de dados têm de notificar as violações de dados que estejam sob a sua responsabilidade às autoridades de controlo, no prazo de 72 horas a contar do momento em que tenham tomado conhecimento das mesmas. Todavia, esta obrigação apenas diz respeito às violações de dados que sejam suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares.

O considerando 87 do RGPD estabelece igualmente que «[h]á que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter especialmente em consideração a natureza e gravidade da violação dos dados pessoais, assim como as respetivas consequências e efeitos adversos para os titulares dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento»[76].

Nesse sentido, se a violação de dados apenas contemplar dados cifrados com uma chave segura[77], ou apenas incluir dados que não apresentem um risco para os seus respetivos titulares, o responsável pelo tratamento não tem de notificar a autoridade de controlo competente.

Na verdade, a obrigação de proceder a tal notificação assenta no pressuposto de existir um risco para os direitos e liberdades das pessoas singulares em causa, segundo o disposto no n.º 1 do artigo 33.º do RGPD. Este regulamento não determina o grau desse risco (se é elevado ou diminuto, por exemplo), pelo que havendo um qualquer risco para os direitos e liberdades dos titulares dos dados, o responsável pelo tratamento deve prontamente efetuar a devida notificação.

---

[75] Cf. artigo 1.º da Regulamento (EU) n.º 611/2013, sobre o âmbito de aplicação do diploma.

[76] Relativamente às competências das autoridades de controlo nesta matéria, veja-se o artigo 51.º e ss. do RGPD.

[77] Por exemplo, uma cifra SHA 512 aos dias de hoje. Cf. PAAR, Christof, PELZL Jan, *Understanding cryptography: a textbook for students and practicioners*, Springer, 2010.

Ora, face à obrigação prevista no n.º 1 do artigo 33.° do RGDP, importa compreender quem é a autoridade de controlo competente, o modo como deve ser feita a notificação e quais os seus termos. Atentemos, portanto, a cada um destes elementos:

1.1. Identificação da autoridade de controlo competente

O RGDP define «autoridade de controlo»[78] como uma autoridade pública independente criada por um Estado-Membro, nos termos do artigo 51.º do mesmo diploma. Em regra, cada Estado-Membro possui uma ou mais autoridades de controlo[79], as quais são competentes para prosseguir as atribuições e exercer os poderes conferidos pelo RGPD no seu próprio Estado-Membro[80].

Portanto, nos casos em que esteja em causa uma violação de proteção de dados num único Estado-Membro, a autoridade de controlo competente será a do lugar do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante. Nos termos do artigo 55.º e ss. do RGPD, as autoridades de controlo possuem competência para exercer os poderes que lhes são conferidos nesse mesmo diploma, no território do seu próprio Estado-Membro[81].

Já nos casos de tratamentos de dados transfronteiriços, dependendo das circunstâncias da violação de dados pessoais, a identificação da autoridade de controlo competente pode ser uma tarefa complexa. Nas situações em que a violação de dados pessoais ocorra em mais do que um Estado-Membro, afiguram-se várias possibilidades quanto à determinação da autoridade de controlo principal com competência em matéria de proteção de dados transfronteiriço, podendo esta ser a respeitante:

- ao estabelecimento principal ou único do responsável pelo tratamento ou do subcontratante (cf. n.º 1 do artigo 56.º do RGPD); ou
- ao Estado-Membro onde exclusivamente tenha tido lugar a violação de dados (mesmo que não seja o lugar do estabelecimento principal do responsável pelo tratamento) ou apenas em cujo Estado-Membro os titulares dos dados tenham sido substancialmente afetados (cf. n.º 2 do artigo 56.º do RGPD).

[78] Cf. n.º 21 do artigo 4.º do RGPD.

[79] Cf. Lista de autoridades de proteção de dados na EU disponível em: http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=50061.

[80] Cr. N.º 1 do artigo 55.º do RGPD.

[81] Apenas a título marginal, cumpre destacar que o texto do número 3 do artigo 55.º do RGPD exclui a competência das autoridades de controlo no controlo de tratamentos de dados efetuados por tribunais no exercício da sua função jurisdicional. Tal facto deve-se ao princípio da separação de poderes consagrado na Constituição da república portuguesa, para que não haja ingerências entre os poderes legislativo, executivo e jurisdicional. Cf. MIRANDA, Jorge, Manual de Direito Constitucional, 3.ª Edição, Tomo IV Coimbra Editora, 2000.

A relevância desta questão prende-se com o facto de a determinação da autoridade de controlo principal competente ser o único interlocutor do responsável pelo tratamento ou do subcontratante no tratamento transfronteiriço (cf. n.º 6 do artigo 56.º do RGPD).

Na verdade, as autoridades de controlo não estão obrigadas pelo RGPD a notificar as suas congéneres noutros países. Contudo, poderá ser relevante adotar um procedimento de comunicação entre as diversas autoridades de controlo em matéria de proteção de dados, quer ao abrigo dos artigos 56.º (Competência da autoridade de controlo principal) e 60.º (Cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas) ou do artigo 61.º (Assistência mútua) do RGDP. A este respeito, cumpre ainda referir que em Portugal a autoridade de controlo é a Comissão Nacional de Proteção de Dados[82], sem prejuízo de as autoridades judiciárias e os órgãos de polícia criminal procederem às investigações que entenderem necessárias.

1.2. Prazo para a notificação

Impende sobre o responsável pelo tratamento a obrigação de notificar a violação de dados pessoais que tenha sofrido à autoridade de controlo competente sem demora injustificada e, sempre que possível, nas 72 horas seguintes ao momento em que tenha tido conhecimento da mesma (cf. n.º1 do artigo 33.º do RGPD).

Nos termos do artigo 33.º do RGDP, importa definir o momento em que o responsável pelo tratamento tenha «tido conhecimento» da violação de dados pessoais, para se poder estabelecer o prazo de 72 horas. A este respeito, o Grupo do Artigo 29 / atual Comité Europeu para a Proteção de Dados entendeu que o responsável pelo tratamento toma conhecimento da violação de dados pessoais quando tiver um grau de certeza razoável de que ocorreu, de facto, um incidente que comprometeu a proteção de dados pessoais[83].

Todavia, a tomada de conhecimento da violação de dados pelo responsável pelo tratamento tem de ser vista casuisticamente. Apenas após a análise de cada uma das violações de dados é que se pode determinar quando é que o responsável tomou verdadeiramente conhecimento desse incidente. Aliás, pode haver situações em que é difícil determinar o momento exato em que que o responsável toma conhecimento das violações de dados. Por exemplo, deve considerar-se a tomada de conhecimento de um incidente de violação de dados quando o engenheiro informático de uma empresa suspeita de um ataque aos servidores da sua empresa ou quando comunica essa informação aos órgãos com poder decisão da mesma?

---

[82] Cf. artigos 21.º e 22.º da LPD.

[83] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827 p. 10 e ss.

Tomando como ponto de partida a dúvida acima colocada, podemos admitir que o responsável pelos serviços informáticos de uma empresa queira averiguar a ocorrência da violação ainda antes de iniciar qualquer procedimento de comunicação interna. Neste caso, apenas após a recolha de evidência que demonstre a violação de dados pessoais é que houve uma efetiva tomada de conhecimento. Pode haver situações em que não é exatamente claro o momento da tomada de conhecimento. Em qualquer caso, entendemos que a violação de dados pessoais deve ser levada ao conhecimento dos órgãos de direção ou com poder de decisão do responsável pelo tratamento. Todavia, não podem ser adotadas manobras dilatórias para evitar a sua tomada de conhecimento. Nesse sentido, devem ser ministradas formações que promovam a sensibilização de todos os colaboradores para a rápida deteção e reporte de suspeitas de violações de dados ao encarregado de proteção de dados do responsável pelo tratamento, como melhor veremos adiante.

O prazo concedido aos responsáveis pelo tratamento de 72 horas após a tomada de conhecimento pretende dar a possibilidade de avaliar o risco para os titulares dos dados e adotar uma resposta adequada à violação. Mesmo que o responsável pelo tratamento tenha uma noção, em abstrato, das implicações da violação – nomeadamente por força de uma avaliação de impacto sobre a proteção de dados (AIPD)[84] realizada previamente –, a avaliação dos danos e circunstâncias concretas tem de ser objeto de uma nova avaliação, à luz da violação de dados pessoais efetivamente observada. Daqui resulta que a AIPD é importante para antever em abstrato os riscos de um determinado tratamento de dados pessoais e adotar medidas de segurança em conformidade, mas não dispensa uma análise casuística do impacto real de uma violação de dados pessoais após a mesma ocorrer.

Dado que o prazo de 72 horas se pode afigurar curto para a tomada de medidas necessárias − entre as quais a notificação à autoridade de controlo competente, a implementação de medidas de controlo de danos, etc. −, entendemos que a existência prévia de um plano operacional de resposta pode ser uma boa prática para agilizar e facilitar a execução de mecanismos internos e de reporte externo, como melhor destacaremos no último capítulo deste trabalho. Deste modo, a fase de reflexão para a estratégia de resposta a adotar será encurtada, já que em grande medida fora antecipada.

A este respeito, importa sublinhar que quando estiverem envolvidos subcontratantes no tratamento de dados pessoais, será também necessário envolvê-los na cadeia de informação e que eles próprios têm o dever de comunicar toda a informação ao responsável pelo tratamento (cf. n.º 2 do artigo. 33.º do RGPD). Uma vez que tanto o responsável como o subcontratante têm a obrigação de implementar as medidas técnicas e organizativas necessárias para a proteção dos dados pessoais[85], ambos devem articular um plano estratégico de resposta face a violações de dados pessoais.

[84] Cf. artigo 35.º e seguintes do RGPD.

[85] Cf. n.º 1 do artigo 32.º do RGPD.

Por último, é de notar que quando o responsável pelo tratamento não puder notificar a autoridade de controlo competente dentro do prazo de 72 horas acima referido, a notificação deverá ser acompanhada dos motivos do atraso[86].

Neste âmbito, importa também sublinhar a possibilidade da comunicação faseada das informações necessárias e constantes n.º 3 do artigo 33.º − e que veremos adiante com detalhe − à autoridade de controlo competente, quando não seja possível prestá-las de imediato[87].

1.3. Responsabilidade pela notificação às autoridades competentes

No que concerne à responsabilidade pela notificação da violação de dados pessoais às autoridades competentes, cumpre averiguar quem é que a deve efetuar. Vejamos, então, as diferentes realidades fáticas.

a) Tratamento de dados efetuado exclusivamente pelo responsável pelo tratamento

Quando o responsável pelo tratamento de dados atua sozinho, não soçobram dúvidas quanto à sua exclusiva responsabilidade pela notificação da violação de dados pessoais.

b) Responsabilidade conjunta pelo tratamento de dados

Sempre que a responsabilidade pelo tratamento de dados for conjunta, os responsáveis conjuntos pelo tratamento de dados deverão idealmente estipular qual é a entidade com a incumbência de notificar a autoridade de controlo competente em caso de violação de dados pessoais[88]. Contudo, na eventualidade de não terem sido determinadas quaisquer disposições contratuais a este respeito entre os responsáveis conjuntos pelo tratamento, não poderá qualquer um deles furtar-se à obrigação de notificar uma violação de dados pessoais da qual tome conhecimento.

Os responsáveis conjuntos pelo tratamento devem coordenar a melhor estratégia para comunicarem entre si as violações de dados pessoais de que algum(uns) deles tenha sido alvo. Pese embora o RGPD não determine especificamente a obrigação de informar os demais responsáveis conjuntos pelo tratamento sobre as violações de dados pessoais de que tomem conhecimento, tal comunicação parece ser do interesse de todos. Nessa medida, os responsáveis conjuntos pelo tratamento poderão antecipar futuros ataques de que potencialmente venham a ser alvo e proceder à notificação à autoridade de controlo competente a uma só voz.

[86] Cf. n.º 1 *in fine* do artigo 33.º do RGPD.

[87] Cf. n.º 4 do artigo 33.º do RGPD.

[88] Cf. Considerando 79 e artigo 26.º do RGPD.

Mesmo inexistindo uma concertação quanto ao responsável conjunto líder no que respeita à notificação da autoridade de controlo, será sempre preferível haver duas ou mais notificações à autoridade de controlo competente a não haver nenhuma.

c) Subcontratantes

O RGPD apresenta como novidade, entre outras, o facto de os subcontratantes poderem ser diretamente responsabilizados pelo tratamento de dados[89]. A título de exemplo podemos constatar a possibilidade de pedidos de indemnização contra o responsável pelo tratamento ou um subcontratante diretamente – sem prejuízo de entre eles ser intentada uma ação de regresso em função do seu grau de responsabilidade.

De acordo com a alínea f) do n.º 3 do artigo 28.º do RGPD, o subcontratante está obrigado a prestar assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações relativas às notificações de violações de dados pessoais à autoridade de controlo com competência.

Nessa senda, também o considerando 82 prescreve que «[a] fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento».

De igual modo, o subcontratante encontra-se obrigado a notificar as violações de dados pessoais de que tome conhecimento ao responsável pelo tratamento, sem demora injustificada[90]. Todavia, a obrigação de notificar a autoridade de controlo cabe ao responsável pelo tratamento e não ao subcontratante, nos termos do n.º 1 do artigo 33.º do RGPD.

1.4. Conteúdo e forma da notificação

A notificação à autoridade de controlo competente deve conter, nos termos do n.º 3 do artigo 33.º do RGPD, no mínimo:

a) uma descrição da natureza da violação dos dados pessoais, incluindo as categorias e o número aproximado de titulares de dados afetados, assim como as categorias e número aproximado dos dados pessoais em causa, se possível;
b) o nome e contactos do encarregado de proteção de dados ou outra pessoa de contacto junto da qual possam ser obtidas mais informações;
c) uma descrição das consequências prováveis da violação de dados pessoais;

[89] Cf. Considerando 13 e artigo 79.º (Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante) do RGPD.

[90] Cf. n.º 2 do artigo 33.º do RGPD.

d) uma descrição das medidas adotadas ou propostas pelo responsável pelo **tratamento para reparar a violação** de dados e/ou mitigar os seus efeitos negativos.

Embora não seja taxativamente indicado no artigo 33.º do RGPD que esta notificação deve ocorrer por escrito, é aconselhável que o seja, sem prejuízo de um reporte por outro meio que permita uma resposta mais expedita por parte da autoridade de controlo competente.

Refira-se que cada autoridade de controlo competente pode exigir um meio próprio para a notificação de violações de dados pessoais. Acresce que o n.º 5 do artigo 33.º do RGPD dispõe que o responsável pelo tratamento tem de documentar quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada, nada é referido quanto à notificação à autoridade de controlo *per se*. No entanto, para mais facilmente provar que o responsável pelo tratamento cumpriu o seu dever de notificação nos termos do artigo 33.º, é aconselhável que esta comunicação seja feita por escrito.

Nesse sentido, no quadro da política de proteção de dados ou num outro documento, deve ser previsto um procedimento para a comunicação de violações de dados pessoais, que identifique aprioristicamente a autoridade de controlo com competência e os seus contactos, assim como o meio/formulário para efetuar essa notificação, caso as autoridades de controlo competentes não exijam um formulário específico.

Algumas autoridades de controlo exigem que este tipo de notificações lhes seja efetuado por via de um formulário próprio, em geral, por via eletrónica[91]. No caso de a autoridade de controlo não possuir um meio específico para a notificação de violação de dados pessoais, o responsável pelo tratamento deve adotar um formulário que cumpra os requisitos descritos no artigo 33.º do RGPD. Preferencialmente, este formulário deve ser claro, com perguntas e respostas sucintas e preenchido pelo EPD ou por alguém com conhecimentos na área da proteção de dados. A ENISA disponibilizou um formulário nas recomendações sobre a implementação técnica do artigo 4.º da Diretiva 2002/58/CE[92], que pode ser adaptado às notificações de violações de dados pessoais noutras áreas para além das telecomunicações[93].

Em relação a Portugal e às violações de dados pessoais em que a autoridade de controlo competente seja a Comissão Nacional de Proteção de Dados, o responsável pelo tratamento de dados pessoais deve proceder à sua notificação através do formulário disponibilizado no website desta instituição[94]. Outras autoridades de controlo disponibilizam outros canais de comunicação, pelo que é aconselhável que os responsáveis pelo tratamento verifiquem antecipadamente qual ou quais as autoridades de

[91] Por exemplo, a autoridade de proteção de dados do Luxemburgo, de Portugal, etc.

[92] Cf. Recommendations on technical implementation guidelines of Article 4, ENISA, 2012, disponíveis em: https://www.enisa.europa.eu/publications/art4_tech.

[93] Cf. Idem, anexo A, p. 48.

[94] Cf. o *website* da CNPD disponível em: www.cnpd.pt.

controlo competente(s) relativamente aos tratamentos de dados que operam e os meios que adotam para as notificações de violações de dados.

1.5. Orientações do Grupo de trabalho do Artigo 29.º / Comité Europeu para a Proteção de Dados

No quadro da sua missão, o CEPD avança algumas medidas práticas em matéria de notificações de violações de dados pessoais destinadas aos responsáveis pelo tratamento de dados e seus subcontratantes[95]:

- identificação de uma pessoa ou equipa com a incumbência de dar uma resposta a este tipo de incidente e a avaliar os riscos envolvidos;
- avaliação do risco para os titulares dos dados na sequência da violação de dados e informação às secções relevantes da organização;
- notificação à autoridade supervisora competente e eventualmente aos titulares dos dados (como continuaremos a analisar);
- medidas de contenção e recuperação dos dados;
- documentação de todos os procedimentos.

Do nosso ponto de vista, entendemos que todas as propostas do CEPD devem ser integralmente adotadas pelos responsáveis pelo tratamento. Entre as medidas *supra* descritas, o maior desafio reside na avaliação do risco pelo responsável pelo tratamento. Contudo, acreditamos que a intervenção do EPD e de uma equipa de suporte é crucial para o responsável pelo tratamento responder às violações de dados pessoais e cumprir com a obrigação de notificar a autoridade de controlo competente sobre as mesmas.

Recordemos que uma violação de dados pessoais pode estar dar origem a um processo penal, pelo que toda a documentação e recolha de prova devem atender aos princípios que subjazem ao processo criminal[96]. Nessa medida, este trabalho não ficaria completo sem uma alusão à necessidade de documentação de todos os procedimentos, quer para efeitos de posterior investigação, quer para cumprimento dos requisitos da notificação da violação de dados pessoais à autoridade de controlo competente. Contudo, por se tratar de um tema com uma abrangência muito extensa e merecedor por si só de um estudo em profundidade, não nos alongaremos na questão da documentação dos

[95] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*", de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827, p. 12.

[96] A documentação de todos os procedimentos na sequência de uma violação de dados pessoais é por si só digna de um estudo autónomo. Por se encontrar fora do âmbito deste estudo, não abordaremos esta temática. A este respeito cf. CASEY, Eoghan, Digital Evidence and Computer Crime, Third Edition, Forensic Science, Computers, and the Internet, Academic Press, 2011.

procedimentos, mas teceremos algumas observações a este propósito no Capítulo «IV. Proposta de plano de notificações face a violações de dados».

2. Notificação aos titulares dos dados pessoais

Ainda antes de descrever as circunstâncias em que é exigida a notificação dos titulares dos dados, atentemos à razão subjacente a esta obrigação. Na verdade, o RGPD apresenta uma especial preocupação com a capacitação e o fortalecimento dos poderes dos titulares dos dados desde o momento da recolha da sua informação pessoal até mesmo às situações de violações de dados pessoais. Tal facto é espelhado em vários artigos, nomeadamente no dever de informação do responsável pelo tratamento (cf. artigos 13.º e ss. do RGPD), no enfoque do consentimento informado (cf. artigos 7.º e ss. do RGPD), etc., e também no artigo 34.º do RGPD sob a epígrafe "Comunicação de uma violação de dados pessoais ao titular dos dados". A necessidade de maior transparência dos tratamentos de dados pessoais – em especial quando os tratamentos de dados pessoais são operados com um grande desequilíbrio de informação entre o responsável e o titular dos dados – encontra-se na génese da obrigação de notificar os titulares dos dados afetados por uma violação de dados pessoais.

Vejamos agora os casos em que é necessária a notificação dos titulares dos dados, para além da notificação da autoridade de controlo competente, como *supra* visto. Para o efeito, seguiremos a mesma estrutura do subcapítulo anterior.

2.1 Identificação dos titulares dos dados lesados dignos de notificação

De acordo com o n.º 1 do artigo 34.º do RGPD, "[q]*uando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada*". Analisando este dispositivo legal, constatamos que contém alguns conceitos indeterminados, designadamente a «**suscetibilidade de** a violação **implicar»** um «**elevado risco» e «sem demora injustificada»**.

Deste modo, diferentemente da análise do risco efetuada pelo responsável pelo tratamento para apurar a necessidade de notificação da violação de dados à autoridade de controlo competente − que não exige um grau mínimo de risco −, a notificação aos titulares dos dados afetados apenas é obrigatória nos casos em que o risco para os seus direitos e liberdades é elevado.

Para melhor compreendermos os conceitos em análise, atentemos novamente na norma ISO 31000:2009 – *Risk management – principles and guidelines* [97]. Em termos gerais, o risco pode ser definido como a possibilidade de uma ameaça explorar uma vulnerabilidade de um ativo que pode

[97] Cf. *International Standard ISO 31000 Risk management – Principles and guidelines, first edition 2009-11-15*.

resultar num prejuízo para a organização ou sistema com impacto na atividade ou negócio. Portanto, o risco é medido pela probabilidade da sua ocorrência e pelo seu impacto.

Assim, imediatamente após tomar conhecimento da violação de dados pessoais de que foi alvo, o responsável pelo tratamento deve simultaneamente executar uma avaliação do risco para os direitos e liberdades dos titulares dos dados e tentar conter esse incidente e os seus efeitos. Só através dessa avaliação do risco é que conseguirá determinar quais as medidas de resposta adequadas e se é ou não necessária a notificação dos titulares dos dados em causa.

Ademais, o n.º 3 do artigo 34.º do RGPD enumera alguns casos em que a notificação ao titular dos dados não é necessária, designadamente se:

- o responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, aos dados pessoais afetados pela violação de dados pessoais, tornando-os incompreensíveis para as pessoas não autorizadas a aceder aos mesmos, como a cifragem;
- o responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar;
- a notificação implicar um esforço desproporcionado, caso em que apenas se exige uma comunicação pública ou outra medida análoga através da qual os titulares dos dados sejam informados de forma igualmente eficaz.

Neste âmbito, compete ao responsável pelo tratamento demonstrar que se encontram observados um ou mais dos critérios acima elencados.

Ainda neste âmbito, importa referir que os representantes legais dos titulares de dados menores também têm de ser notificados. Esta comunicação deverá ser ponderada, nos casos em que implique um esforço desproporcionado, nos termos da alínea c) do artigo 3 do artigo 34.º do RGPD. A título de exemplo, se for detetada uma violação de dados de indivíduos entre os dezasseis e os dezoito anos de idade, que aderiram a uma determinada rede social e que não indicaram nenhum contacto dos seus representantes legais, então, parece que a notificação apenas a estes titulares cumprirá os requisitos do RGPD, desde que seja adotada uma linguagem adequada a esta faixa etária, como veremos adiante no subcapítulo «2.4 Conteúdo e forma da notificação».

Por fim, cumpre apenas sublinhar que as violações de dados não suscetíveis de implicar um elevado risco para os direitos e liberdades dos seus titulares não têm de lhes ser notificadas. Contudo, é pertinente referir que em determinadas circunstâncias será oportuno que o responsável pelo tratamento tranquilize as pessoas cujos dados pessoais não foram afetados pela violação de dados, para garantir a sua confiança no tratamento de dados que operam.

2.2 Prazo para a notificação

O n.º 1 do artigo 34.º do RGDP não estipula um prazo exato para a notificação da violação de dados aos titulares de dados afetados, contrariamente à notificação à autoridade de controlo − a qual, como vimos, deverá ocorrer nas 72 horas após a tomada de conhecimento da violação de dados. O articulado apenas indica que a notificação aos titulares dos dados deve ocorrer "**sem demora injustificada".**

Como visto, a notificação aos titulares dos dados não está dependente da notificação prévia às autoridades de controlo competentes, do ponto de vista temporal. Já vimos que sempre que seja necessária a notificação dos titulares dos dados é também necessário notificar a autoridade de controlo com competência em matéria de violação de dados pessoais. Contudo, o Considerando 86 do RGPD prescreve que a comunicação aos titulares dos dados deve ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Portanto, entendemos que pode ser favorável a notificação à autoridade de controlo competente antes da notificação dos titulares, na medida em que aquela poderá providenciar orientações pertinentes para a notificação dos segundos.

Aliás, o n.º 4 do artigo 34.º do RGPD estabelece que a autoridade de controlo pode exigir a notificação da violação de dados pessoais aos titulares dos dados, considerando a probabilidade de a mesma resultar num elevado risco para os mesmos, quando o responsável pelo tratamento ainda não a tiver comunicado. Igualmente na mesma disposição normativa, a autoridade de controlo competente pode aferir se as condições previstas no n.º 3 do artigo 34.º do RGPD se encontram observadas.

Por fim, cumpre mencionar o Considerando 88 do RGPD quando refere que a notificação de violações de dados deve atender aos legítimos interesses das autoridades de polícia, nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais. Deste modo e nos casos aplicáveis, a notificação à autoridade de controlo competente, bem como aos órgãos de polícia criminal deve ter lugar previamente à notificação dos titulares dos dados. Assim, o plano de notificações deverá contemplar a aferição do envolvimento das autoridades competentes em matéria de investigação criminal, ou seja, dos órgãos de polícia criminal (OPC), a par das autoridades nacionais de proteção de dados pessoais. Nessa medida, a notificação aos titulares dos dados poderá ser diferida, em função das necessidades de investigação criminal e da preservação da prova, sem prejuízo de estes virem a ser informados logo que possível.

Não iremos abordar esta questão em profundidade, por se tratar de um tema que extravasa o âmbito deste estudo. No entanto, uma vez que a intervenção de OPC pode ter impacto no prazo de notificação das violações de dados pessoais aos titulares dos dados, não poderíamos deixar de a mencionar neste trabalho.

Acresce referir que nas situações em que o responsável pelo tratamento não disponha dos contactos dos titulares dos dados, a informação sobre a violação de dados deve ser prestada quando for possível.

A título de exemplo, quando os próprios titulares exerçam o direito de acesso ou contactem o responsável pelo tratamento.

2.3 Responsabilidade pela notificação

Nos termos do n.º 1 do artigo 34.º do RGPD, cabe ao responsável pelo tratamento a obrigação de notificar os titulares dos dados quando a violação de dados pessoais ofereça uma suscetibilidade de implicar um elevado risco para os direitos e liberdades dessas pessoas singulares. De acordo com essa disposição legal, o responsável pelo tratamento terá de avaliar a necessidade a notificação dos titulares de dados afetados em função do risco para os seus direitos e liberdades.

Reitere-se, todavia, que a notificação à autoridade de controlo é sempre necessária nestes casos, dado que a obrigação de notificação das violações de dados aos respetivos titulares contém mais requisitos legais, como vimos. Portanto, em caso de dúvida, o responsável pelo tratamento poderá fazer a ponderação da necessidade de notificação dos titulares dos dados em conjunto com a autoridade de controlo competente, se assim o entender.

2.4 Conteúdo e forma da notificação

O n.º 2 do artigo 34.º do RGPD indica qual o conteúdo mínimo da notificação aos titulares dos dados quando uma violação de dados pessoais seja suscetível de implicar um elevado risco para os seus direitos e liberdades. Nesse sentido, esta comunicação deverá, numa linguagem clara e simples, descrever a natureza da violação dos dados pessoais e facultar as informações e medidas previstas nas alíneas b), c) e d) do n.º 3 do artigo 33.º do RGPD:

- o **nome e contactos do encarregado de proteção de dados** ou de outro ponto de contacto através do qual possam ser obtidas mais informações;
- as **consequências prováveis da violação** de dados;
- as **medidas adotadas ou propostas** pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus efeitos negativos.

No entanto, nada impede que o responsável pelo tratamento ofereça mais informações sobre a violação de dados pessoais. A este respeito, cumpre também notar que as comunicações de violações de dados aos titulares devem atender aos seus conhecimentos, maturidade e língua. Portanto, descrições demasiado técnicas, que não sejam inteligíveis ao homem médio, não cumprirão os pressupostos relativos à clareza e simplicidade da notificação descritos no n.º 2 do artigo 34.º do RGPD. A adaptação da linguagem terá também de contemplar os casos em que os titulares dos dados sejam menores. Nestes casos, o texto deverá ser adaptado à faixa etária em causa, sem prejuízo de serem igualmente notificados os seus representantes legais.

O mesmo se diga quanto à língua utilizada para a referida notificação. A comunicação da violação de dados pessoais deve ser feita na mesma língua utilizada nas interações prévias entre aquele indivíduo

e o responsável pelo tratamento. No caso de não existir nenhum contacto prévio, o Grupo de trabalho do Artigo 29.º/ Comité Europeu para a Proteção de Dados entende que deve ser adotada a língua local do titular dos dados, salvo se tal exigir meios excessivos[98]. A razão prende-se com a efetiva compreensão da comunicação de violação de dados pessoais por parte dos titulares dos dados, para que este possa adotar as medidas que entender adequadas face à violação.

As comunicações relativas a violações de dados devem ser autónomas, e não estar associadas a outras informações que o responsável pelo tratamento queira transmitir aos titulares dos dados. Assim, o responsável pelo tratamento não deve, por exemplo, utilizar uma *newsletter* ou fatura dos seus serviços para informar os indivíduos de uma violação de dados pessoais que seja suscetível de constituir um risco elevado para os seus direitos e liberdades.

Estas exigências de autonomização, língua e linguagem das comunicações de violações de dados têm por base o princípio da transparência e a inteligibilidade da informação. De outro modo, o propósito destas notificações de ajudar os titulares dos dados a protegerem-se contra efeitos negativos eventuais e/ou reais decorrentes da violação de dados pessoais seria comprometido.

Como vimos, o RGPD não determina um meio específico para as notificações de violações de dados pessoais aos titulares dos dados afetados. A este respeito, diga-se que o responsável pelo tratamento é quem se encontra mais bem posicionado para determinar qual o canal de comunicação privilegiado com os titulares dos dados, baseado no histórico das comunicações anteriores com os mesmos.

Ainda no que concerne à forma, diga-se que a comunicação pode ter lugar por mais do que uma via. Se o responsável pelo tratamento assim o entender, poderá enviar um email e uma mensagem (*short message service* – SMS) aos destinatários pertinentes, por exemplo.

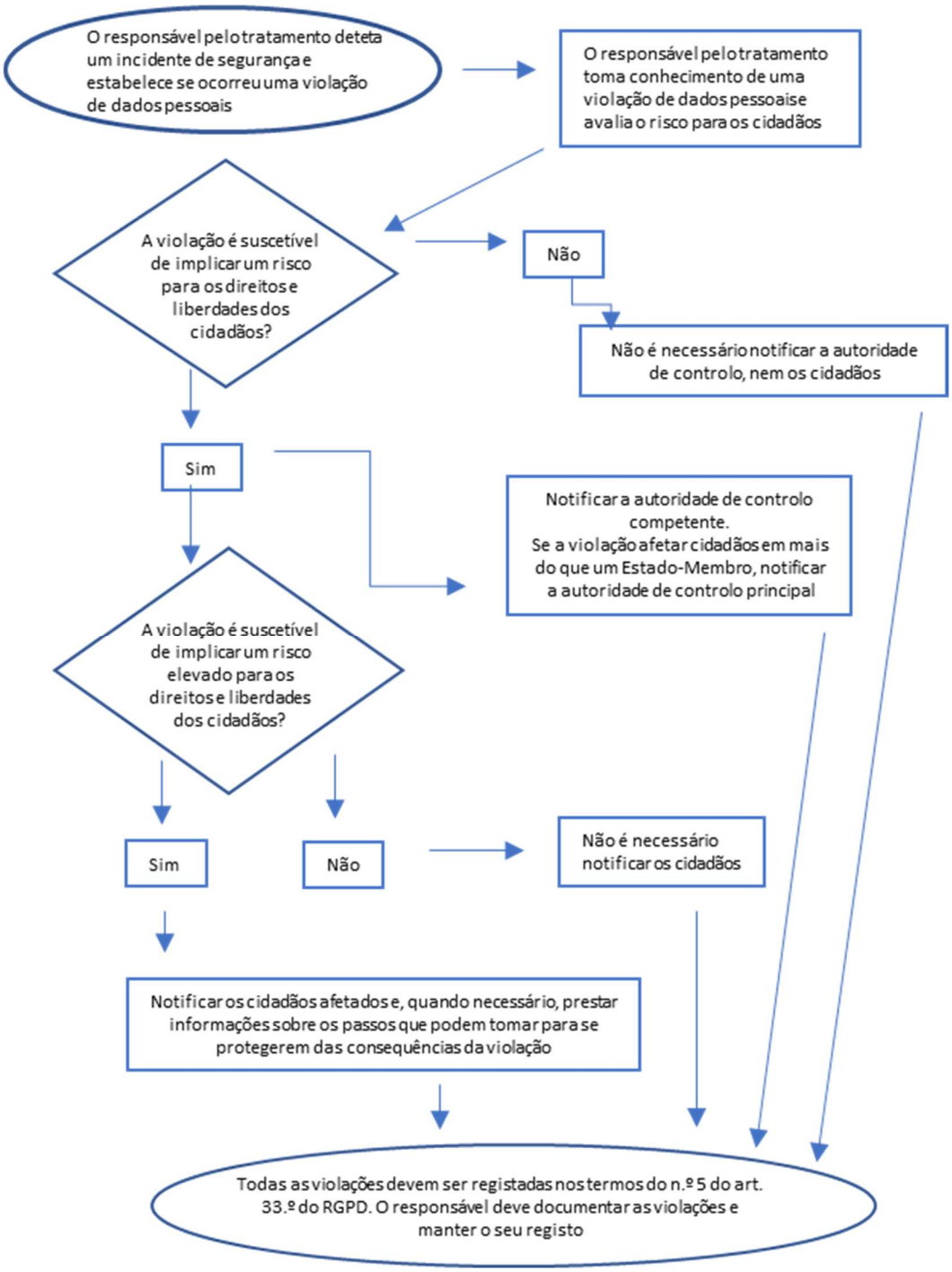
É desejável que a informação seja transmitida individualmente de uma forma clara e inteligível, num formato legível e, preferencialmente, que permita ao responsável pelo tratamento saber se essa notificação foi devidamente rececionada. Todavia, quando a comunicação aos titulares dos dados implique um esforço desproporcionado para o responsável pelo tratamento, este fica dispensado de a fazer individualmente, desde que proceda a uma comunicação pública ou tome outra medida semelhante e igualmente eficaz, nos termos da alínea c) do n.º 3 do artigo 34.º do RGPD.

[98] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827, p. 21.

3. Fluxograma e tabela comparativa de notificações de violações de dados pessoais

Com vista a sumariar as situações em que devem ser notificadas as violações de dados pessoais, traduzimos infra o fluxograma avançado pelo CEPD nas suas orientações[99]:

Figura 1 – Fluxograma do CEPD com os requisitos das notificações de violações de dados pessoais



[99] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827, p. 30.

Para concluir este capítulo e melhor compararmos as semelhanças e diferenças entre o regime de notificações às autoridades de controlo competentes e aos titulares dos dados, tentámos resumir sumariamente os seus principais aspetos na tabela *infra*.

Figura 2 – Tabela comparativa entre as notificações de violações de dados pessoais às autoridades de controlo e aos titulares dos dados, nos termos dos artigos 33.º e 34.º do RGPD.

	Notificações às autoridades de controlo	**Notificações aos titulares dos dados**
FUNDAMENTO LEGAL	Artigo 33.º do RGPD	Artigo 34.º do RGPD
IDENTIFICAÇÃO DO(S) DESTINATÁRIO(S)	Autoridade de controlo com competência nos termos do artigo 55.º do RGPD	Pessoas singulares cuja violação dos dados pessoais for suscetível de implicar um elevado risco para os seus direitos e liberdades
PRAZO	Até 72 horas após o responsável pelo tratamento ter tido conhecimento da violação de dados pessoais	Sem demora injustificada
RESPONSABILIDADE PELA NOTIFICAÇÃO	Responsável pelo tratamento de dados	
CONTEÚDO	• Descrição da natureza da violação dos dados pessoais; • nome e contactos do encarregado de proteção de dados (ou outra pessoa de contacto); • descrição das consequências prováveis; • descrição das medidas adotadas ou propostas.	

4. Responsabilidade e regime sancionatório pelo incumprimento das notificações de violações de dados pessoais

Uma vez que as notificações de violações de dados pessoais são uma obrigação imposta pelo RGPD aos responsáveis pelo tratamento nos termos dos artigos 33.º e 34.º, o seu incumprimento implica a aplicação das sanções previstas igualmente nesse regulamento.

Assim, caso os titulares dos dados afetados considerem que o tratamento dos seus dados pessoais incumpriu uma das disposições do RGPD – como a não notificação de uma violação de dados pessoais, etc. – podem apresentar uma reclamação junto da autoridade de controlo competente, nos termos do artigo 77.º do RGPD. Esta reclamação não prejudica o facto de poderem intentar uma ação judicial contra os responsáveis pelo tratamento, nos termos do artigo 79.º o RGPD. Por outro lado, os titulares dos dados podem igualmente recorrer a vias extrajudiciais, como os julgados de paz, para fazerem exercer o seu direito à proteção de dados.

O regime sancionatório do RGPD tem sido bastante falado devido à previsão no n.º 5 do artigo 83.º da possibilidade de aplicação de coimas de valores elevados (até 20.000.000€ ou, no caso de uma empresa, até 4% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado) por parte das autoridades de controlo[100].

Portanto, se o responsável pelo tratamento tomar conhecimento de uma violação de dados pessoais com impacto nos direitos e liberdades dos titulares desses dados e não a comunicar à autoridade de controlo, nos termos do artigo 33.º do RGPD, está a incumprir a legislação. Se o responsável for alvo de uma violação de dados pessoais, mas não tomar conhecimento dessa violação, então, não há um incumprimento relativamente à obrigação de notificar essa violação.

Nos casos de responsabilidade conjunta (cf. artigo 26.º do RGPD), basta que um dos responsáveis pelo tratamento tome conhecimento da violação de dados pessoais para se iniciar o prazo de 72 horas respeitante à notificação da violação de dados à autoridade de controlo.

Relativamente aos subcontratantes, a alínea f) do n.º 3 do artigo 28.º do RGPD dispõe que o subcontratante deve prestar assistência ao responsável pelo tratamento no sentido de assegurar as notificações previstas nos artigos 33.º e 34.º do mesmo diploma. Adicionalmente, o n.º 2 do artigo 33.º prevê a obrigação de os subcontratantes notificarem o responsável pelo tratamento relativamente às violações de dados pessoais de que tomem conhecimento. Nessa medida, caso não cumpram essa obrigação, podem ser sancionados por violação dos seus deveres.

Por último cumpre assinalar que o artigo 84.º do RGPD permite que os Estados-Membros estabeleçam regras relativamente a outras sanções aplicáveis em caso de violação do disposto no próprio regulamento. Esta remissão para a legislação interna permite que sejam aplicadas outras sanções, as quais terão de ser materializadas em diplomas nacionais.

[100] Atendendo aos valores em causa, alguns responsáveis pelo tratamento consideram vantajoso obterem um seguro para os custos decorrentes de eventuais violações de dados pessoais.

III. Proposta de boas práticas e de um procedimento de comunicações/notificações face a violações de dados pessoais

Face ao descrito nos capítulos anteriores, os responsáveis pelo tratamento de dados, bem como os subcontratantes devem promover uma cultura de prevenção, mas também de comunicação de violações de dados pessoais, com vista a mitigar os seus efeitos adversos, quer para os titulares dos dados, quer para as suas próprias organizações.

Na verdade, as notificações de violações de dados pessoais não podem ser vistas isoladamente, dado que a sua rápida deteção contribuirá também para a célere notificação às autoridades de controlo. Nesse sentido, é recomendável a adoção de um plano de resposta a violações de dados pessoais por parte dos responsáveis pelo tratamento. Este plano irá forçosamente implicar o emprego de tempo, de recursos humanos e financeiros e, mas acreditamos que a planificação adequada não só mitigará eventuais riscos, como também garantirá um retorno seguro desse investimento.

Acresce que os recursos humanos e financeiros das micro-empresas, pequenas e médias empresas (PME) e grandes empresas é diferente, apresentando reflexos na abordagem de comunicação de violações de dados pessoais. Sem prejuízo das diferenças inerentes à escala, tentaremos neste capítulo elencar um conjunto de boas práticas e tecer um plano de notificações face a violações de dados pessoais que seja exequível por todas as entidades (responsáveis pelo tratamento, subcontratantes e seus representantes), independentemente da sua dimensão. Por fim, apresentaremos as conclusões de um estudo de caso, no qual foi aplicada a nossa proposta de procedimento de notificações de violações de dados pessoais.

1. Boas práticas

Podemos elencar um conjunto de boas práticas que facilitam os processos de notificação de violações de dados pessoais para os responsáveis pelo tratamento. No entanto, estas boas práticas não podem cingir-se ao momento da notificação das violações de dados pessoais às autoridades de controlo, já que esta implica uma avaliação do risco, uma descrição dos dados e das categorias dos titulares de dados afetados, assim como o conhecimento de conceitos prévios (adoção de medidas de segurança adequadas, proteção de dados desde a conceção e por defeito, etc.). Por essa razão, numa perspetiva holística, tentaremos apresentar boas práticas com um reflexo direto na notificação de violações de dados pessoais – tanto às autoridades de controlo, como aos titulares dos dados afetados.

Na verdade, para que sejam cumpridos os prazos para as notificações e com o conteúdo que é exigido pelo RGPD – e que analisámos no capítulo II deste trabalho – é necessário que os responsáveis pelo tratamento e os subcontratantes estejam conscientes das suas responsabilidades e tenham adotado as medidas técnicas e organizativas adequadas ao tratamento de dados pessoais que operam – e não apenas relativamente ao procedimento de notificação de violações de dados. Simultaneamente, devem ser definidas as cadeias de comunicação internas e externas e identificadas as pessoas, junto das

quais a informação sobre as violações de dados pessoais deve circular. A este respeito, as orientações do CEPD sobre violações de dados pessoais no quadro do RGPD[101] são elucidativas quanto aos casos em que as autoridades de controlo devem ser notificadas, mas não abordam os procedimentos prévios que permitem detetar e, consequentemente, notificar as autoridades de controlo e os titulares dos dados dentro dos prazos determinados no RGPD. Ora, tentaremos neste capítulo descrever uma proposta de procedimento de notificações/comunicações de violações de dados pessoais que os responsáveis pelo tratamento podem adotar internamente no quadro dos seus procedimentos de rotina. Entendemos que esta proposta facilita o cumprimento dos requisitos de notificação das violações de dados pessoais impostos pelo RGPD aos responsáveis pelo tratamento.

De ressalvar também que os procedimentos de mitigação do impacto das violações de dados devem atender a possíveis investigações por parte das autoridades de controlo ou de órgãos de polícia criminal, pelo que a recolha atempada da prova deve estar presente na planificação da resposta a incidentes de segurança que contendam com violações de dados pessoais.

Vejamos, então, as boas práticas que devem ser adotadas pelos responsáveis pelo tratamento com maior detalhe.

1.1 Planificação e adoção de uma política de proteção de dados

Uma resposta rápida e eficaz ante uma violação de dados pessoais, incluindo a sua notificação às autoridades de controlo e titulares dos dados afetados, requer uma planificação prévia e adequada. No âmbito do conceito da proteção de dados desde a conceção, há muitas vantagens na adoção de uma política de proteção de dados.

Ora, uma política de proteção de dados trata-se de um documento que prevê as normas, métodos, procedimentos e instruções – tanto a nível estratégico, como tático e operacional –, com o objetivo de assegurar a manutenção e sistematização/normalização da segurança, bem como o cumprimento da legislação em matéria de proteção de dados. Esta política deve atender não só aos aspetos orgânicos da organização, como também às condições humanas e tecnológicas.

Consciente das suas vantagens, o legislador europeu previu no n.º 2 do artigo 24.º do RGPD que as medidas de segurança técnicas e organizativas adequadas ao tratamento de dados pessoais efetuado pelo responsável pelo tratamento incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento, caso sejam proporcionadas face às atividades do tratamento de dados.

Ora, o principal objetivo de uma política de proteção de dados é proporcionar aos colaboradores de uma organização uma correta orientação e auxílio no cumprimento dos requisitos exigidos para um ou

[101] Cf. *Guidelines on Personal data breach notification under Regulation 2016/679*", de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018, disponíveis em: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827.

vários tratamentos de dados pessoais. Para tanto, afigura-se relevante que a mesma tenha em consideração as especificidades do seu negócio/atividade, as potenciais ameaças, a situação geopolítica, as fragilidades e os aspetos fortes da organização. Desse modo, uma política de proteção de dados deve aproximar-se de uma política de segurança, ao identificar a informação e os ativos sensíveis (como as categorias especiais de dados), garantir as propriedades de segurança, definir as responsabilidades de todos os envolvidos na mesma, estabelecer as prioridades de implementação e promover uma cultura de segurança. No entanto, tem também de atender às obrigações impostas pela legislação de proteção de dados, prevendo procedimentos de deteção, reporte, mitigação de efeitos e notificação de violações de dados pessoais, por exemplo.

Nesse sentido, para desenhar uma política de proteção de dados devem *a priori* ser pensadas quatro premissas:

a) a sua **arquitetura**, ou seja, o modo como é estruturada a política, o tipo de dados pessoais que devem ser considerados, quem a deve desenvolver (exigindo-se um compromisso entre o EPD, os técnicos de informática, os gestores da organização e, por fim, todos os colaboradores a quem compete executar a política);
b) o **controlo**, que obriga à fiscalização de que as normas e procedimentos da política são efetivamente observados, bem como que se mantêm atuais face aos desenvolvimentos tecnológicos, à legislação e até ao modelo de negócio/atividade;
c) a **responsabilidade**, permitindo que aqueles que não cumprem a política de proteção de dados sejam chamados à colação por esse facto, mas assentando num princípio de confiança; e
d) a **aplicabilidade**, que respeita à implementação e exequibilidade das normas, métodos e procedimentos.

Assim, a política de proteção de dados deve ser estabelecida por escrito, preferencialmente através de um documento emanado pelos órgãos superiores da hierarquia das organizações, conferindo-lhe assim a importância que a mesma deve merecer junto de todos os colaboradores. Este documento de alto nível deve ser redigido de um modo claro e sucinto, indicando o *modus operandi* do acesso e tratamento dos dados pessoais, assim como as regras, restrições e responsabilidades dos diferentes utilizadores. Deve igualmente procurar uma perspetiva geral e abstrata, aplicável a todos os colaboradores e com uma visão tecnologicamente neutra e realista – que não careça de frequentes atualizações, nem comprometa a sua exequibilidade.

Com vista à aplicação efetiva da política de proteção de dados, é necessário que o seu conteúdo seja divulgado a todos os utilizadores que manuseiam dados pessoais – o que, na prática, pode implicar todos os departamentos e unidades da organização. A segurança e a proteção de dados são uma responsabilidade de todos, pelo que se impõe uma difusão transversal da informação relevante, nomeadamente da política de proteção de dados. Nesse sentido, são adequadas ações de formação, *newsletters* e secções de perguntas frequentes (*Frequently Asked Questions* - FAQ) nos *website* e Intranet das organizações com a possibilidade permanente de consulta da política de proteção de dados, para que haja uma sensibilização, responsabilização e envolvimento de todos os destinatários.

Atendendo ao facto de a política de proteção de dados ser o primeiro nível de defesa de uma organização, não é demais reforçar que quanto maior o grau de detalhe, maior a probabilidade de sucesso da sua efetiva aplicação por todos os seus destinatários, ou seja, pelas chefias, mas também pelos departamentos técnicos de informática e por todos os demais colaboradores.

Tendo presente o acima exposto, aquando da elaboração de uma política de proteção de dados devem ser atendidos os seguintes aspetos:

a) Definição clara da finalidade da política de proteção de dados: se os colaboradores não compreenderem a razão da adoção de determinados procedimentos, o seu grau de adesão aos mesmos será muito inferior;
b) Estipulação das responsabilidades: não basta elencar em termos genéricos os deveres que assistem aos colaboradores de uma organização. É necessário concretizar as responsabilidades específicas de cada um;
c) Delimitação do âmbito da política de proteção de dados: é tão pernicioso aplicar procedimentos excessivos a matérias que não carecem dessa proteção, como desatender a procedimentos de segurança necessários à segurança da informação verdadeiramente sensível. Nesse sentido, é importante classificar e definir os dados pessoais na política de proteção de dados;
d) Observância das normas jurídicas: a política de proteção de dados internas deve ir ao encontro da legislação aplicável (RGPD, etc.);
e) Estipulação de um regime sancionatório: todos os visados devem estar cientes das consequências que resultam da violação da política de proteção de dados;
f) Menção de documentos complementares: todos os documentos que suportem a informação vertida na política de proteção de dados e que estejam diretamente relacionados com a mesma devem ser referidos;
g) Identificação dos procedimentos a adotar em caso de comunicação de incidentes: a política de proteção de dados não deve limitar-se à prescrição de procedimentos preventivos, devendo igualmente definir os procedimentos em caso de violação de dados pessoais, incluindo a sua notificação às autoridades de controlo e aos titulares dos dados afetados;
h) Definição do procedimento de revisão e de monitorização: uma vez que a política de proteção de dados não deve ser um documento estático, mas antes um documento que acompanha as necessidades das organizações e a evolução tecnológica, é pertinente proceder à sua revisão periódica, mesmo que apenas para validar o seu conteúdo anterior;
i) Estipulação da data da revisão: a periodicidade da revisão deve atender ao constante progresso tecnológico, sem cair no excesso de implicar uma burocracia exagerada para a sua permanente atualização. É aconselhável uma revisão anual, sem prejuízo de a mesma ter lugar sempre que se justifique (devendo tal facto ser estipulado na própria política de proteção de dados);
j) Definições terminológicas e de conceitos fundamentais: para evitar ambiguidade na interpretação de conceitos-chave, deve a política de proteção de dados claramente definir os termos que emprega no seu texto. Todavia, aconselha-se a adoção de definições alinhadas

com o disposto no RGPD e noutros documentos legislativos, em vez da mera remissão para os mesmos. Deste modo, a leitura do documento torna-se mais clara e dispensa a consulta de outros documentos por motivos definitórios;

k) Estipulação de exceções: em Direito sabemos que «não há regra sem exceção». Todavia, as regras gerais, mas também as exceções aplicáveis devem ser transpostas para a política de proteção de dados, reduzindo a discricionariedade da atuação dos seus destinatários e garantindo uma maior uniformidade da sua aplicação;
l) Identificação do autor da política de proteção de dados: por uma questão de transparência, mas também para atribuição do estatuto de documento de alto nível. Recomenda-se que seja da autoria do EPD, dado o seu grau de especialidade nesta matéria, sem prejuízo de ser da autoria de outra pessoa com idênticas competências;
m) Identificação do responsável que autorizou a política de proteção de dados: a autoridade e validade da política de proteção de dados é reafirmada pela identificação do responsável que a autorizou;
n) Identificação do responsável por fazer cumprir a política de proteção de dados: para efeitos da sua implementação, pode ser necessário contactar o responsável pela execução da mesma. Esta responsabilidade deverá ser assumida pelo EPD, no caso de ser nomeado um;
o) Data da aprovação da política de proteção de dados: permite aferir o momento a partir do qual é vinculativa a sua aplicação;
p) Identificação da entidade a contactar em caso de dúvidas: facilita e centraliza a resolução de problemas e a resposta a dúvidas dos destinatários da política de proteção de dados. Uma vez mais, deverá ser o EPD a desempenhar esta função, na eventualidade de ser nomeado um pelo responsável pelo tratamento;
q) Delimitação da responsabilidade institucional: circunscreve a responsabilidade da organização, designadamente face a eventos que não estejam na sua esfera de controlo. É, também por isso, um reconhecimento de que a segurança e proteção de dados não depende unicamente da implementação de uma política com esse escopo. Contudo, não pode o responsável pelo tratamento furtar-se às obrigações que lhe são impostas pelo quadro normativo vigente.

Analisados o conteúdo e a importância de uma política de proteção de dados, vejamos qual a sua relevância no âmbito das notificações de violações de dados pessoais. De facto, para que haja uma pronta notificação de uma violação de dados pessoais às autoridades de controlo competentes é necessária uma rápida deteção dessa mesma violação, bem como o acionamento de um plano de comunicações e aferições internas com intervenientes expressamente definidos. Nesse sentido, o responsável pelo tratamento de dados deve contemplar uma política de proteção de dados que inclua a preparação, a deteção, a contenção, a investigação, a mitigação, a recuperação e a notificação das violações de dados pessoais[102].

[102] A divisão de resposta a incidentes de segurança em seis fases é proposta pelo Computer Security Incident Handling Guide do National Institute of Standards and Technology/U.S. Department of Commerce, disponível em:

Pese embora a adoção de uma política de proteção de dados pareça fora do âmbito da temática das notificações de violações de dados, na verdade, está na sua génese. Importa que os responsáveis pelo tratamento considerem uma visão holística das ações de prevenção, mitigação e recuperação de violações de dados pessoais, para que haja coerência em todo o seu espectro. Deste modo e para a obtenção de resultados mais eficazes, os responsáveis pelo tratamento devem desenhar um procedimento de resposta a violações de proteção de dados dentro da política de proteção de dados. Ora, sublinhe-se que esta política deverá ter em conta os princípios e normas constantes do RGPD. Portanto, atendendo nomeadamente ao princípio da responsabilidade (cf. n.º 2 do art. 5.º do RGPD), ressalva-se a obrigação de o responsável pelo tratamento cumprir com a legislação vigente, mas também de demonstrar que está efetivamente a cumpri-la.

A este propósito, não é despiciendo recordar o disposto no artigo 30.º do RGPD, o qual refere no seu n.º 1 que cada responsável pelo tratamento, ou o seu representante, deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade, contendo designadamente:

- O nome e contactos do responsável pelo tratamento e do EPD, se aplicável;
- A finalidade do tratamento de dados;
- A descrição das categorias de titulares de dados e das categorias de dados pessoais;
- As categorias de destinatários a quem os dados pessoais foram ou serão divulgados;
- As transferências de dados para países terceiros, se aplicável;
- Os prazos de conservação dos dados, se possível;
- A descrição geral das medidas técnicas e organizativas adotadas para a segurança dos dados pessoais, se possível.

Em suma, uma política de proteção de dados deverá atender à natureza dos tratamentos de dados efetuados pelo responsável pelo tratamento, bem como a todas as categorias de dados pessoais, categorias de destinatários, aos riscos, etc., como *supra* visto no capítulo II deste estudo. Para tanto, terá de conter não só os princípios gerais, como os procedimentos que operacionalizam a implementação da privacidade desde a conceção e por defeito (art. 25.º RGPD), entre outros.

Para assegurar a sua constante atualização, a política de proteção de dados deve periodicamente efetuar controlos técnicos e organizacionais mínimos para a gestão do risco. Os riscos e o seu impacto variam de acordo com os tratamentos de dados efetuados, a evolução tecnológica, fatores organizacionais internos e externos, pelo que é imperativa a sua análise, bem como a adequação das medidas de resposta e, consequentemente da própria política de proteção de dados. Nesse sentido, o n.º 1 in fine do artigo 24.º do RGPD vem impor que as medidas de segurança técnicas e organizativas sejam revistas e atualizadas consoante as necessidades.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Entendemos que todas estas fases são igualmente relevantes para as notificações de violações de dados pessoais.

1.2 Plano de resposta a incidentes de segurança

As violações de dados pessoais, como muitas vezes já referido neste trabalho, requerem uma estratégia holística, que inclua a sua prevenção, a sua rápida detenção, as notificações obrigatórias pela legislação vigente, a mitigação do seu impacto e a aprendizagem que permita otimizar as medidas de segurança aplicadas aos tratamentos de dados pessoais e evitar a repetição de incidentes. Por uma questão de limitação de tempo e impossibilidade de analisar com a devida profundidade todos os aspetos acima enunciados, o enfoque deste estudo circunscreve-se às notificações de violações de dados pessoais. Todavia, temos de evidenciar como uma boa prática a adoção um plano de resposta a incidentes de segurança[103] e de procedimentos de notificações de violações de dados.

A este respeito, a norma de certificação da *International Organization for Standardization (ISO), Information technology – Security techniques – Information security incident management, Part 1: Principles of incident management* (ISO/IEC 27035-1:2016) é um bom exemplo. No fundo, esta norma estabelece uma abordagem estruturada para as diversas fases da gestão de incidentes relativos à segurança da informação:

a) Plano e preparação;
b) Deteção e avaliação;
c) Notificação e resposta;
d) Recolha de prova e análise forense;
e) Revisão e melhoria contínua.

Independentemente das orientações previstas na norma ISO/IEC 27035-1:2016, os responsáveis pelo tratamento podem adotar um plano de resposta a incidentes de segurança utilizando esta divisão faseada. Desse modo e focando-nos nas questões relativas às notificações de violações de dados pessoais – sem prejuízo de serem também abordados outros tópicos no plano de resposta a incidentes de segurança –, podemos incluir na primeira fase a política de proteção de dados pessoais *supra* descrita. Esta compreende os procedimentos de notificação de violações de dados pessoais, a par da designação de um EPD e da formação/sensibilização para a proteção de dados de todos os recursos humanos. Relativamente à fase b), a deteção de possíveis violações de dados pessoais e a avaliação da sua gravidade e impacto são os aspetos mais relevantes. Prosseguindo este paralelismo entre o objeto deste estudo e as fases de um plano de resposta a incidentes de segurança, a notificação às autoridades de controlo e aos titulares de dados afetados, quando aplicável, insere-se na fase c). Inclui-se igualmente nesta fase a adoção de medidas de mitigação das possíveis consequências negativas para os titulares dos dados. A documentação dos procedimentos, a recolha de prova e comunicação aos OPC caberá na fase d). Por fim, com vista a garantir a otimização de processos, procedimentos e

[103] Cf. European Network and Information Security Agency (ENISA), Good Practice Guide for Incident Management, 2010, disponível em: http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management.

metodologias, o responsável pelo tratamento deverá analisar se os riscos foram efetivamente controlados e adotar as melhores práticas para que a situação de violação de dados pessoais não volte a ocorrer, a que corresponde a fase e).

Não se ignora que as violações de proteção de dados pessoais são apenas um dos vários incidentes de segurança que podem ocorrer. Todavia, estas merecem a devida atenção dentro de um plano de resposta a incidentes de segurança devido ao potencial impacto que podem implicar para os titulares dos dados pessoais potencialmente afetados.

1.3 Adoção de medidas de segurança técnicas e organizativas

A adoção de medidas de segurança técnicas e organizativas adequadas para assegurar e comprovar a conformidade do tratamento de dados pessoais é uma obrigação do responsável pelo tratamento, segundo o disposto no n.º 1 do artigo 24.º do RGPD. Estas medidas podem reduzir o risco de violações de dados pessoais, mas também facilitar a rápida deteção de violações de dados. Nos termos do princípio da responsabilidade, compete ao responsável pelo tratamento apurar quais as medidas técnicas e organizativas adequadas e implementá-las (cf. n.º 2 do artigo 5.º e n.º 1 do artigo 24.º do RGPD). Para tanto, a realização de avaliações de impacto sobre a proteção de dados (cf. artigo 35.º do RGPD), a consulta prévia das autoridades de controlo com competência em matéria de proteção de dados (cf. artigo 36.º do RGPD), assim como do EPD (cf. artigo 37.º e ss do RGPD) podem ser relevantes.

Todavia, não é possível determinar as medidas de segurança adequadas de um modo geral para todos os tratamentos. O nível de segurança apropriado tem de ser aferido em relação ao risco e, portanto, avaliado casuisticamente para cada tratamento de dados pessoais. Importa, por isso, sublinhar que a adequação das medidas de segurança técnicas e organizativas irá depender do tratamento de dados pessoais em causa, do seu responsável pelo tratamento, de circunstancialismos internos e externos, não existindo uma «receita única» para os responsáveis pelo tratamento. Consequentemente, a tónica da adequação recai sobre a proporcionalidade das medidas de segurança aplicadas face aos circunstancialismos de cada tratamento de dados pessoais. Com vista a melhor concretizar o conceito de medidas de segurança técnicas e organizativas, iremos referir *infra* alguns exemplos, pese embora não se trate de uma lista exaustiva.

Sendo a segurança e a proteção de dados pessoais elementos fundamentais à boa gestão, exige-se o envolvimento de todos os intervenientes – e não apenas das chefias ou órgãos dirigentes –, dado que todos terão de aplicar medidas de segurança, seja através de processos administrativos, operações, comunicações, etc. Por essa razão, a par da definição de uma **política de segurança** (com as respetivas medidas de segurança técnicas e organizativas), a organização terá de apostar numa **política de comunicação**, na qual os colaboradores e utilizadores sejam devidamente informados e estejam conscientes das suas responsabilidades, do funcionamento do sistema de informação e dos protocolos, políticas e regulamentos de segurança. Com o propósito de melhor transmitir a informação,

todos os **procedimentos e protocolos devem ser claros e materializados por escrito**, garantindo uma regulação e comunicação uniforme, assim como a produção de registos fiáveis. Complementarmente, a **formação contínua** ajudará a manter estes conceitos presentes e a atualizar procedimentos e medidas de segurança que se revelem menos eficazes.

Continuando a promover uma cultura de segurança e de proteção de dados das organizações, a aplicação do princípio da minimização dos dados deve estar transversalmente presente no tratamento de dados, o que significa que apenas devem ser recolhidos e tratados os dados pessoais verdadeiramente necessários.

Como já referido, as medidas de segurança ajudam a mitigar os riscos. Desse modo, para avaliar em que medida e de que modo deve ser implementada a estratégia de segurança, terá de ser ponderada a **gestão do risco**, sob a perspetiva do custo-benefício, mas também atendendo à sensibilidade da informação. Nesse sentido, deverá de ser definido um **perímetro de defesa**, que controle o fluxo de informação entre a Intranet e a Internet, ou seja, entre os utilizadores legítimos e terceiros. Deste modo, a proteção contemplará possíveis ataques provenientes do interior, mas também do exterior de uma organização.

Por conseguinte, no sentido de escalonar o acesso à informação, deverá de ser estruturado um sistema que identifique e permita o acesso em função do perfil de utilizador. Para tanto, a **definição das permissões de acesso** só poderá ser determinada após uma análise das **necessidades de acesso** de cada colaborador/categoria profissional e da **classificação da informação** em vários níveis, de acordo com o seu grau de confidencialidade. Contudo, a atribuição de permissões de acesso deve ter presente que um determinado nível de credenciação não justifica por si só a obtenção de acesso a toda a informação desse nível, se não for necessária. Na mesma senda, deve ser implementado um sistema de *logs* de acesso, com auditorias periódicas para detetar e controlar prontamente acessos indevidos.

Na sequência da definição das permissões de acesso acima descrita, no que concerne ao **controlo de acessos**, deverá ser estruturada a hierarquia de acessos, garantindo uma correta **separação de funções**, assim como que todos os colaboradores tenham apenas acesso à informação que necessitam para o desempenho da sua atividade profissional (**princípio do mínimo privilégio** com base no **princípio da necessidade**). Nesse sentido e para assegurar a **independência do controlo**, recomenda-se que o responsável pelo desenho, implementação e operação do sistema, não seja o Administrador do sistema.

Ainda no âmbito da prevenção, deverá ser implementado um **sistema de identificação pessoal** com dois suportes distintos obrigatórios (e não opcionais), como por exemplo através da utilização de uma chave eletrónica e de um registo biométrico. O facto de o sistema se basear em duas fontes distintas reduz o risco de roubo de identidade e de acessos indevidos.

A **separação dos dados** é outra das medidas a implementar para garantir uma estratégia de segurança eficaz, que evita simultaneamente a centralização da informação e, consequentemente, do seu acesso.

Para tanto, é necessária a prévia classificação da informação e a aplicação de filtros que identifiquem rótulos de segurança para aceder à informação. Em complemento desta medida, deve ser aplicada a **compartimentação** da informação, na medida em que restringe e isola o acesso à informação, reduzindo o risco de comprometimento da informação classificada como confidencial.

No sentido de assegurar a confidencialidade, a **utilização de cifras** – tanto para proteger a informação transmitida, como a informação guardada – é um mecanismo adicional de segurança, ainda que não seja absolutamente inviolável. Com o mesmo intuito, podem igualmente aplicar-se técnicas como a pseudonimização ou anonimização. A título exemplificativo, o acesso indevido a dados pessoais cifrados com um algoritmo seguro de acordo com o estado da arte não comporta os mesmos riscos que uma violação de dados pessoais não cifrados. No entanto, o acesso indevido a dados cifrados continua a ser uma violação de dados, que carece da respetiva documentação interna pelo responsável pelo tratamento. A diferença reside no facto de os efeitos negativos serem mitigados com a cifragem e, nessa medida, não serem suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares, ficando dispensada a notificação às autoridades de controlo, nos termos do n.º 1 do artigo 33.º do RGPD. Se, por um lado, a confidencialidade, a integridade e a disponibilidade não forem colocadas em causa com a violação de dados, então não estamos perante uma situação que mereça a notificação das autoridades de controlo e dos titulares dos dados, uma vez que não parece existir um risco para os direitos e liberdades das pessoas singulares. Por outro lado, se a violação de dados cifrados consistir na perda irrecuperável de dados pessoais, tal significa que as medidas de segurança aplicadas não foram adequadas e, portanto, cumpre notificar as autoridades de proteção de dados competentes, caso haja um risco para os direitos e liberdades dos titulares dos dados.

Ainda no âmbito da confidencialidade, a utilização de **certificados digitais**, em particular no que respeita à comunicação de dados, é uma solução que combina o controlo de acesso, a autenticação, o não repúdio e a integridade da informação, através de uma entidade certificadora e de registo que, mediante políticas e procedimentos de segurança, aplica um *time-stamping* à informação.

No quadro da transmissão e comunicação de informação sensível, a aplicação de uma **infraestrutura de chave pública** (*Public Key Infrastructure*)[104] é uma solução a ser ponderada para a informação de acesso reservado.

Já no que respeita à preservação da integridade da informação, a aplicação de assinaturas digitais e de **funções de Hash**, que codificam a informação, deverão ser medidas a adotar. Relativamente aos ataques exteriores, considera-se essencial a implementação de ***firewall***. Contudo, para determinada informação de natureza mais sensível, e dada a interatividade dos sistemas e redes envolvidos, poderá ser ainda necessário adotar um regime de **defesa em profundidade**. A vantagem da defesa em profundidade reside no aumento da proteção mediante a criação de várias camadas de acesso, através

[104] PAAR, Christof e PELZL, Jan, "*Understanding Cryptography, A Textbook for Students and Practitioners*", Springer, 2010.

de um conjunto de operações, procedimentos e equipamentos, em vez de um único sistema de segurança.

Atendendo ao facto de a informação poder estar em diversos suportes – como *hardcopy*, *softcopy*, conhecimento pessoal, conhecimento corporativo, videoconferências e chamadas telefónicas, etc. – também a estratégia de segurança terá de contemplar estes vários formatos, sem prejuízo da sua manutenção em ***back-ups***.

Como vimos *supra*, a **segurança lógica** – acautelada nomeadamente através de *scanners* de vírus, controlos de acesso, gestão de contas, arquitetura securitária, redes virtuais privadas (VPN - *Virtual Private Network*) –, terá de ser conjugada com a **segurança física**, por exemplo através de câmaras de videovigilância, do controlo de entradas por vigilantes, do armazenamento da informação reservada em armários com chave ou cofres, etc.

Importa igualmente assegurar a **disponibilidade dos dados pessoais** através da definição de planos de emergência – como a negação dos acessos após uma falha –, de continuidade de operações e de manutenção preventiva. A prevenção não deve limitar-se à mera antecipação de eventuais ataques para formular protocolos que tentem evitar a sua concretização, mas também antever hipoteticamente a sua efetiva realização, pelo que os planos de emergência e de continuidade de operações são primordiais. Por outro lado, o controlo de acessos, o encerramento de falhas conhecidas nos sistemas operativos e na configuração de rede e a adoção de procedimentos para recuperação de dados (como os *back-ups*) são práticas a ter também em consideração na planificação de uma estratégia de segurança da informação e de proteção de dados.

Por fim, para garantir que a política de proteção de dados, bem como os seus regulamentos, protocolos e procedimentos estão a ser cumpridos, é fundamental que sejam realizadas **auditorias internas e externas**, de modo a que haja uma avaliação global da eficácia das medidas de segurança e do nível de cumprimento.

Em suma, a **diversidade das medidas de segurança** será a melhor estratégia para prevenir eventuais falhas ou ataques que coloquem em risco o direito fundamental à proteção de dados, pese embora as organizações devam estar conscientes de que não existe nenhuma política de proteção de dados ou de segurança absolutamente infalível.

Ademais, um mesmo tratamento de dados pessoais pode requerer medidas de segurança diferentes em função da sua localização. Para ilustrar esta hipótese, tomemos como exemplo um responsável pelo tratamento cuja sede e servidores informáticos se encontram localizados numa zona de cheias fluviais. Neste cenário, não é recomendável que os servidores sejam alojados na cave, mas antes em zonas menos propícias a serem afetadas por intempéries.

Acresce que, atendendo à lei de Moore, o custo da tecnologia diminui a um ritmo muito acelerado, contribuindo a diminuição do preço da tecnologia em idêntica medida para que os custos com os ciberataques decaiam e, consequentemente, aumente a sua complexidade. Assim, é patente a

pertinência da proteção de dados pessoais, exigindo das organizações uma constante atenção e preocupação com as novas ameaças aos seus sistemas de informação.

Cumpre ainda dizer que após a tomada de conhecimento de uma violação de dados pessoais, podem ser implementadas novas medidas de segurança. A título de exemplo, atente-se na aplicação de um período de «quarentena» no acesso às bases de dados de uma empresa.

1.4 Códigos de conduta e mecanismos de certificação

A adoção de códigos de conduta ou de mecanismos de certificação que contribuam para a correta aplicação do RGPD está prevista nos artigos 40.º e 41.º deste mesmo regulamento. Por um lado, a certificação e os códigos de conduta permitem harmonizar eventuais diferenças existentes entre os vários Estados-Membros. Por outro, permitem assegurar que determinados requisitos mínimos sejam implementados, quer no *software*, quer no *hardware*, quer na estrutura da organização, etc., independentemente da ação ou inação dos utilizadores/titulares dos dados pessoais. Deste modo, o nível mínimo de proteção de dados é elevado para um padrão superior, alavancando este direito fundamental para um nível de proteção que oferece mais garantias do que os requisitos mínimos legais.

Os códigos de conduta e/ou processos de certificação dos sistemas de gestão da segurança da informação (doravante SGSI) permitem uma análise e avaliação das organizações nas suas várias temáticas, na medida em que atendem a determinados fatores que têm impacto na sua segurança. Por um lado, a certificação pode definir os riscos envolvidos, propondo um SGSI, que implementa uma estrutura organizacional para a segurança da informação, assim como determina os processos, tecnologias e responsabilidades em causa. Deste modo, ao definir determinados objetivos concretos, a certificação e os códigos de conduta mitigam eventuais danos provocados por acidentes e facilitam a implementação dos controlos de segurança.

O processo de certificação apresenta ainda como vantagens o facto de formalizar os processos de segurança da informação e a respetiva documentação, assim como de identificar o risco para a organização e a sua gestão, ajudando ainda a identificar os requisitos regulamentares da contratação.

Vimos anteriormente neste subcapítulo a certificação *International Organization for Standardization (ISO), Information technology – Security techniques – Information security incident management, Part 1: Principles of incident management* (ISO/IEC 27035-1:2016). No entanto, existem outras certificações relevantes e pertinentes a respeito da segurança da informação e violações de dados pessoais.

A certificação ISO/IEC 27000 é composta por diversas normas e consiste num modelo de referência internacional para o estabelecimento, implementação, operacionalização, monitorização, análise crítica e melhoria de um SGSI. Deste modo, ao padronizar e definir os requisitos para um SGSI de uma organização, a certificação alcança os objetivos da segurança da informação, ou seja, a preservação da sua confidencialidade, integridade e disponibilidade através da aplicação de um processo de gestão

de riscos. Por outro lado, protege a confiança das partes interessadas, assegurando que os riscos são geridos de forma adequada e uniforme (estandardizada).

A norma ISO/IEC 27001:2013 *Information technology -- Security techniques -- Information security management systems -- Requirements* tem como racional 4 fases (o ciclo "PDCA - Plan, Do, Check, Act") que permitem planear, gerir, controlar/monitorizar e agir face ao SGSI. Analisando autonomamente cada uma das secções da norma, constatamos as principais linhas orientadoras que a norteiam.

A Secção 4 da certificação ISO 27001:2013, denominada *Contexto da Organização*, dispõe sobre a identificação de todas as partes interessadas e os seus requisitos de segurança. Analisa também os condicionalismos que influenciam a capacidade de proteção da organização.

Já a Secção 5 *Liderança* versa sobre a gestão de topo, a qual deve ser comprometida e revelar capacidade. É nesta secção que é também indicada a política e os objetivos (ou modelo de referência para a sua definição) que regulam a comunicação, as funções, a responsabilidade e autoridade atribuídas, bem como o apoio e orientação que as chefias têm de evidenciar.

Na Secção 6 *Planeamento* determinam-se os riscos e oportunidades, para evitar ou reduzir efeitos indesejáveis, assim como para implementar ações, avaliações e análises de risco. Pretende-se com estas medidas a Declaração de Aplicabilidade (controlos/objetos implementados e justificados com os do ANEXO A da norma), a aprovação de um plano para o tratamento de riscos e para a implementação de objetivos de segurança da informação, identificando o seu modo, momento de implementação e responsável. No fundo, são antevistas as ações para responder aos riscos e às oportunidades da organização no que respeita à segurança da informação, bem como são traçados os objetivos da segurança da informação e qual o caminho para alcançá-la.

Na Secção 7, dedicada ao *Suporte*, são estipulados os recursos necessários, as competências, a comunicação e consciencialização. Indica-se como a informação deve encontrar-se documentada, atualizada e sistematizada de forma apropriada, nos termos indicados pela norma, respeitando também as normas da organização e cumprindo eventuais requisitos exigidos pela natureza da própria informação. Indicam-se igualmente os complexos processos e interações, assim como se revela uma especial preocupação com o controlo da informação.

Na Secção 8 *Operação*, o enfoque incide sobre o planeamento e controlo operacional, ou seja, sobre os processos, a avaliação de risco em intervalos regulares ou quando necessário, os resultados das avaliações e o plano de tratamento de risco.

Já na Secção 9 a norma dispõe sobre a *Avaliação do Desempenho*, ao definir o que deve ser avaliado, medido e controlado, quais os métodos que permitem a produção de resultados comparáveis e reproduzíveis, quais os intervenientes nessa avaliação e como aferir os resultados das monitorizações. Nesta secção, indicam-se ainda os critérios e o âmbito das auditorias internas, assim como os relatórios

a apresentar superiormente, nos quais devem ser identificadas as oportunidades de melhoria, fundamentando os resultados a apresentar para a revisão pela gestão da organização.

Por fim, na Secção 10 dedicada à *Melhoria,* descreve-se a atuação face à avaliação de não conformidades, devendo ser alterado o SGSI, caso seja necessário. Assim, identificam-se quais os procedimentos a adotar no sentido da correção dos aspetos menos positivos identificados na avaliação ou auditoria, com vista à melhoria contínua.

Existem outras certificações e estão a ser desenvolvidos diversos processos de certificação da segurança da informação, atendendo às novas disposições do RGPD. Abstemo-nos de uma avaliação das melhores certificações e não pretendemos fazer um levantamento exaustivo dos vários processos de certificação existentes com pertinência em matéria de violações de dados pessoais. Contudo, os dois exemplos de certificações acima referidos, tal como muitos outros, são evidências de boas práticas pelos responsáveis pelo tratamento e contribuem para o cumprimento dos requisitos previstos no RGPD.

1.5 Avaliação bifásica do impacto da violação de dados pessoais após a sua tomada de conhecimento

Em 2012, a ENISA estabeleceu várias recomendações[105] para as empresas de telecomunicações na sequência das obrigações de notificação de violações de dados impostas pela Diretiva relativa à privacidade e às comunicações eletrónicas[106] – atualmente em fase de revisão pelo legislador europeu[107].

Ora, como anteriormente referido, o RGPD veio estabelecer esta obrigação, ainda que com algumas nuances, para todos os responsáveis pelo tratamento, nos termos dos seus artigos 33.º e 34.º. Portanto, algumas das recomendações da ENISA destinadas aos operadores de telecomunicações podem e devem ser adotadas *cum grano salis* pelos responsáveis pelo tratamento de outras áreas. Entre estas recomendações, encontramos a avaliação bifásica da violação de dados pessoais. Nesse sentido, o responsável pelo tratamento deve promover junto do EPD a realização de uma avaliação da violação de dados pessoais nas 24 horas após a tomada de conhecimento da mesma pelo responsável pelo tratamento, assim como uma outra avaliação mais detalhada aproximadamente 48 horas após essa

[105] Cf. Recommendations on technical implementation guidelines of Article 4, ENISA, 2012, disponíveis em: https://www.enisa.europa.eu/publications/art4_tech.

[106] Cf. Diretiva 2002/58/CE, DIRECTIVA 2002/58/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas), posteriormente alterada pela Diretiva 2009/136/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 25 de Novembro de 2009.

[107] Cf. Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas) de 10.01.2017, disponível em: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42693.

tomada de conhecimento, que permita uma análise da sua gravidade e impacto com a maior acuidade possível.

Ambas as análises devem incidir sobre os critérios constantes do RGPD, ou seja, a natureza da violação de dados, as categorias e números de titulares afetados, as categorias e número de registos de dados pessoais envolvidos, as consequências prováveis da violação de dados, as medidas adotadas ou propostas para cessar e mitigar os efeitos da violação de dados, o grau de impacto para os titulares dos dados afetados, etc.. A diferença entre as duas avaliações da violação de dados decorre do espaço temporal entre ambas, o qual permite a recolha de um maior número de elementos na segunda avaliação. Consequentemente, como serão apuradas mais informações graças ao maior tempo de investigação e de recolha de informação, o grau de detalhe de cada uma das avaliações será diferente.

A avaliação inicial permitirá confirmar se o incidente reportado se trata de uma efetiva violação de dados pessoais, bem como delineará uma visão preliminar do potencial impacto e gravidade da violação de dados. Nesta fase, o responsável pelo tratamento de dados deverá identificar a causa e autor da violação, a natureza/tipologia da violação de dados, os titulares dos dados afetados e a uma estimativa da gravidade da violação[108]. Ainda que não seja possível determinar o grau exato da gravidade da violação, esta estimativa possibilitará a tomada de medidas concretas dirigidas a cessá-la – caso esta ainda se mantenha – e a mitigar alguns dos seus efeitos adversos.

Diferentemente, a segunda avaliação será o resultado de uma análise mais extensiva e profunda, capaz de retratar melhor a realidade. Esta análise deve ter presente a avaliação inicial da violação de dados pessoais, mas será mais detalhada devido ao maior tempo de investigação. Nesse sentido, as circunstâncias e o impacto da violação serão mais fundamentados e a avaliação da gravidade da violação será mais rigorosa. A ENISA apresenta a seguinte escala[109] para avaliar o impacto geral de uma violação de dados pessoais:

Figura 3 – Escala de avaliação do impacto geral de violações de dados (ENISA)

[108] A ENISA disponibiliza uma escala para determinar a gravidade de uma violação de dados pessoais nas *Recommendations on technical implementation guidelines of Article 4*, ENISA, 2012, Anexo B, p. 53 e ss.

[109] Cf. Idem, p. 23 e ss.

Escala para avaliação do impacto geral		
Pontuação geral	Avaliação	Efeitos adversos
1	Baixa/ negligenciável	Inexistentes ou negligenciáveis
2-3	Média	Não muito sérios e podem ser ultrapassados
4-5	Elevada	Consideráveis/ sérios, mas podem ser ultrapassados com algum esforço
6-7	Muito elevada	Extremamente sérios, requerendo um esforço significativo para os eliminar ou com possíveis consequências permanentes que não podem ser ultrapassadas pelas pessoas afetadas

Legenda: Escala para avaliação do impacto geral de violações de dados pessoais proposta pela ENISA na Recomendações sobre linhas orientadoras da implementação técnica do artigo 4.º (Recommendations on technical implementation guidelines of Article 4).

A principal vantagem deste sistema de avaliação bifásico reside no facto de o responsável pelo tratamento poder tomar decisões informadas e medidas reativas à violação de dados pessoais nas 24 horas seguintes à sua tomada de conhecimento (curto prazo), assim como avaliar a sua eficácia posteriormente (entre as 48 horas e as 72 horas após a tomada de conhecimento da violação de dados), ainda antes de notificar a autoridade de controlo.

Ambas as avaliações beneficiarão de um sistema de gestão de risco focado na proteção de dados pessoais e na identificação de potenciais impactos para os titulares dos dados – e não apenas no risco para a continuidade da atividade ou para a organização em causa –, se o responsável pelo tratamento o tiver implementado. Deste modo, o responsável pelo tratamento poderá melhor prevenir, detetar e reagir às violações de dados pessoais. Por todas estas razões, a notificação à autoridade de controlo competente será baseada nesta segunda avaliação.

Neste âmbito, a ENISA entende que devem constar do processo de gestão do risco os seguintes elementos[110]:

- Identificação e avaliação dos dados pessoais;

[110] Cf. *Recommendations on technical implementation guidelines of Article 4,* ENISA, 2012, p. 14-16, disponíveis em: https://www.enisa.europa.eu/publications/art4_tech.

- Identificação e avaliação das vulnerabilidades e ameaças;
- Identificação e avaliação do risco final e do nível de aceitação do risco;
- Tratamento do risco (redução, transferência e aceitação do risco);
- Como lidar com riscos residuais.

A gestão do risco é um tema que extravasa o âmbito deste trabalho, pelo que não iremos abordar este tema. No entanto, esta análise ficaria incompleta se, pelo menos, não elencasse os elementos da gestão do risco que podem contribuir para a avaliação bifásica após a tomada de conhecimento da violação de dados.

1.6 Investigação e documentação

A problemática da investigação e documentação forenses de violações de dados pessoais – em especial no ciberespaço[111] – é digna de um estudo próprio[112], mas que extravasa o âmbito deste trabalho. Assim, por razões de circunscrição temporal e delimitação do tema deste trabalho não abordaremos esta temática.

No entanto cumpre referir que o responsável pelo tratamento tem de documentar todas as violações de dados pessoais, incluindo as que não requerem uma notificação às autoridades de controlo, designadamente os factos, os efeitos e as medidas de reparação adotadas (cf. n.º 5 do art. 33.º do RGPD). Esta obrigação é um reflexo do princípio da responsabilidade que impende sobre o responsável pelo tratamento (cf. n.º 2 do art. 5.º do RGPD). Para tanto, afigura-se essencial manter um registo das operações de tratamento de dados e informações adicionais pertinentes. Ademais, o n.º 1 do artigo 24.º do mesmo regulamento reitera a obrigação de o responsável pelo tratamento poder comprovar que o tratamento de dados é realizado em conformidade com o RGPD.

De acordo com os n.º 1 e 3 do artigo 33.º do RGPD, no momento da notificação das violações de dados à autoridade de controlo, o responsável pelo tratamento tem de indicar vários elementos sobre as mesmas. De entre os requisitos mínimos elencados no n.º 3 desse artigo, o responsável deve:

- descrever a natureza da violação de dados;
- indicar as categorias e o número aproximado de titulares de dados afetados;
- identificar as categorias e o número aproximado de registos de dados pessoais;
- comunicar o nome e contactos do EPD;
- descrever quais as consequências prováveis da violação de dados pessoais;
- descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar e/ou atenuar os efeitos negativos da violação de dados.

[111] CASEY, Eoghan, Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet, Academic Press, 2011.

[112] Cf, CASEY, Eoghan, Handbook of Digital Forensics and Investigation, Academic Press, 2010.

Todavia, como *supra* referido estes são os requisitos mínimos exigidos pelo RGPD. Tal significa que, caso a autoridade de controlo entenda que devem ser prestadas mais informações ou se for aberto um inquérito judicial, pode ser solicitada informação adicional. Consequentemente, a intervenção dos OPC pode implicar a recolha de elementos complementares.

1.7 Investimento em recursos humanos e materiais para a cabal deteção e reporte das violações de dados pessoais

As violações de dados pessoais podem ser detetadas por alertas automáticos, previamente instalados nos sistemas informáticos, e/ou por colaboradores da organização. Em qualquer dos casos, os responsáveis pelo tratamento têm de empregar recursos humanos e tecnológicos para responder a eventuais violações de dados e, posteriormente, procederem à notificação das mesmas às autoridades de controlo e aos titulares dos dados, quando aplicável.

Antes de prosseguirmos com a análise das boas práticas quanto à estipulação de equipas internas e à nomeação de um encarregado de proteção de dados – a cujas temáticas dedicaremos a nossa atenção mais adiante – cumpre referir que o responsável pelo tratamento deve encarar com seriedade a possibilidade de vir a sofrer uma violação de dados. Tal facto, pode ser comprovado com o grau de minúcia que presta a esta possibilidade e à sua resposta, com a adoção de medidas preventivas de mitigação e reporte, ou com o investimento em recursos humanos e materiais para a cabal deteção e reporte das violações de dados pessoais.

No entanto, não queremos com isto dizer que o responsável pelo tratamento é obrigado a empregar recursos humanos, técnicos e financeiros de valores incalculáveis. Pretendemos apenas sublinhar que os responsáveis pelo tratamento devem possuir um conjunto mínimo de recursos que possam ser alocados à proteção de dados, em função dos tratamentos de dados pessoais que operam. Lembremos que o princípio da proporcionalidade é um dos princípios mais relevantes em matéria de proteção de dados. Por outras palavras, se um responsável pelo tratamento pretender efetuar um tratamento de dados pessoais que inclua categorias especiais de dados, deve contemplar na sua planificação não só os custos com a avaliação de impacto sobre a proteção de dados, mas também com as medidas de segurança técnicas e organizativas adequadas a esse tratamento e com as obrigações de notificações decorrentes de eventuais violações de dados pessoais. Nessa mesma linha de pensamento, os recursos humanos e materiais – incluindo os necessários para a deteção e notificação de violações de dados pessoais – que o responsável pelo tratamento deve empregar têm de ser efetivamente adequados ao tratamento de dados pessoais.

Ora, uma planificação que considere o pior dos cenários possíveis não significa que o responsável pelo tratamento não tem confiança no seu tratamento de dados pessoais e no plano de resposta a uma violação de dados pessoais, mas antes que atendeu a várias possibilidades, incluindo panoramas catastróficos. Aliás, a consideração do pior dos cenários é a melhor forma de garantir que a avaliação do risco foi bem ponderada.

1.8 Nomeação de um Encarregado de Proteção de Dados (EPD) e definição de uma equipa de apoio em violações de dados pessoais

Como vimos, uma das inovações trazidas pelo RGPD é a previsão da designação de um encarregado de proteção de dados (doravante EPD). De acordo com o artigo 37.º e seguintes deste regulamento, a designação de um EPD apenas é obrigatória quando:

- o tratamento de dados pessoais for efetuado por uma autoridade ou organismo público, salvo os tribunais;
- as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações que − devido à sua natureza, âmbito e/ou finalidade − exijam um controlo regular e sistemático dos titulares de dados em grande escala;
- as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações em grande escala de categorias especiais de dados (cf. artigo 9.º do RGDP) ou de dados relacionados com condenações penais e infrações (cf. artigo 10.º do RGPD).

Não obstante o RGDP não exigir a nomeação de um EPD nos demais casos, afigura-se uma decisão avisada nomear um EPD, já que será uma pessoa com capacidade para contribuir para a arquitetura da política de proteção de dados, mas também para auxiliar o responsável pelo tratamento, nos casos de violações de dados pessoais. Se o EPD possuir um conhecimento profundo dos ativos e idiossincrasias dos tratamentos de dados de um determinado responsável, poderá delinear melhor a política de proteção de dados, assim como o plano de comunicação e de mitigação de violações de dados pessoais.

Segundo o RGPD, o EPD deverá possuir um conjunto de competências para executar cabalmente as seguintes funções:

- informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem dados, sobre as suas obrigações;
- controlar a conformidade com o RGPD e outras disposições relativas à proteção de dados;
- aconselhar no que concerne a avaliações de impacto sobre a proteção de dados;
- cooperar com a autoridade de controlo;
- ser o ponto de contacto para a autoridade de controlo em matéria de proteção de dados.

A este respeito, o CEPD emitiu orientações, referindo quais as qualidades profissionais e conhecimentos especializados que um EPD deve possuir para desempenhar todas as funções acima descritas[113]. Dentro dessas competências, encontramos:

- o conhecimento das práticas e legislação nacional e europeia em matéria de proteção de dados;

[113] Cf. Orientações sobre o encarregado de proteção de dados (EPD) do Grupo de Trabalho do Artigo 29.º, revistas e adotadas em abril de 2017, disponíveis em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048.

- a compreensão dos tratamentos de dados pessoais realizados pelo responsável pelo tratamento, bem como das tecnologias de informação e de segurança dos dados; conhecimento do setor e da organização; e
- a capacidade para promover uma cultura de proteção de dados dentro da instituição.

Ao perfil acima elencado, acresce que o EPD atua com confidencialidade e independência (cf. n.º 3, 5 e 6 do artigo 38.º do RGPD), não podendo receber instruções relativamente à proteção de dados no exercício das suas funções, assim como ser destituído ou penalizado pelo responsável pelo tratamento ou subcontratante pelo facto de exercer as suas funções. Adicionalmente, o EPD não pode exercer outras funções ou atribuições que sejam incompatíveis com essa qualidade ou das quais resulte um conflito de interesses (cf. n.º 3 e 6 do artigo 38.º do RGPD).

No que respeita ao plano de comunicação, o EPD poderá coordenar as avaliações do impacto das violações de dados, contando naturalmente com os contributos de todos os colaboradores da organização envolvidos nas mesmas, assim como com as equipas técnicas de informática e de comunicação. De outra banda, o EPD será o contacto privilegiado com as autoridades de controlo com competência em matéria de proteção de dados, com os titulares dos dados afetados e com os OPC. Na linha destas considerações, o EPD será o principal ponto de contacto do responsável pelo tratamento, quer internamente, quer do ponto de vista externo.

Ainda a este respeito cumpre referir que a informação relativa a violações de dados pessoais deve ser tratada com base na necessidade de conhecer (*on a need to know basis*). Nessa senda, o EPD apenas deverá comunicar a informação que for, de facto, necessária e apenas às pessoas e entidades com competência e relevância em tomarem conhecimento das violações de dados pessoais.

Tendo presente estas considerações, é fundamental a definição de uma equipa responsável por violações de dados pessoais e a arquitetura de uma cadeia de comunicação, em primeiro lugar interna e, posteriormente, externa – ou seja, a intervenientes externos ao responsável pelo tratamento de dados pessoais, às autoridades de controlo e aos titulares dos dados afetados, quando aplicável – para o cumprimento dos prazos definidos pelo RGPD.

Sem prejuízo de estabelecermos no subcapítulo seguinte uma proposta de um procedimento de comunicação entre as pessoas chave dentro de uma organização que possam contribuir para a cadeia de comunicações e notificações internas e externas de violações de dados pessoais, não poderíamos deixar de apontar como uma boa prática a definição de uma equipa com capacidade para a centralização do reporte destas eventuais violações. Idealmente, essa equipa deverá ser composta pelo EPD – caso tenha sido designado – ou por outra pessoa com conhecimentos em matéria de proteção de dados pessoais e por pessoas da área das tecnologias da informação de do Direito. A atribuição de competências a esta equipa com nomes definidos permitirá a sua maior responsabilização e eficácia.

Deste modo, graças à centralização das comunicações internas de violações de dados pessoais, é possível tecer uma visão geral da abrangência das violações. Esta visão global ganha ainda mais relevância quando o responsável pelo tratamento dos dados tem diversas sucursais ou filiais, que se encontram igualmente sujeitas aos mesmos riscos[114].

Em todo o caso, para que a informação circule de uma forma ágil, mas apenas pelas pessoas com necessidade de a conhecerem, importa definir aprioristicamente uma equipa de resposta − com competência profissional, recursos financeiros e humanos para o efetivo desempenho das suas tarefas −, mas também quais as autoridades competentes em matéria de proteção de dados pessoais que devem ser notificadas. Uma vez mais, a antecipação dos atores a envolver após a tomada de conhecimento de uma violação de dados pessoais será uma atitude prudente do responsável pelo tratamento e do EPD. Em termos simples, com a pesquisa prévia das entidades a serem notificadas na resposta a uma violação de dados pessoais e a segurança de haver procedido às notificações necessárias, o responsável pelo tratamento e o EPD poderão focar a sua atenção noutros aspetos da resposta a uma violação de dados pessoais.

1.9 Promoção de formação

A formação na área das TIC, mas também em matéria de proteção de dados é fundamental para que todas as pessoas envolvidas no tratamento de dados pessoais possam conhecer melhor os riscos e os procedimentos a adotar no caso de uma violação de dados pessoais. Portanto, a formação contínua dos colaboradores, com um nível de profundidade diferenciado por categorias profissionais ou por outros critérios, atendendo às suas necessidades reais e aos riscos a que se encontram sujeitos, permitirá a sua sensibilização e atualização.

Sabendo que a maioria das violações de dados ocorrem devido a erros humanos[115] ou por via de más práticas dos trabalhadores, acreditamos que a maior sensibilização para a temática da proteção de dados pessoais terá um impacto positivo na sua prevenção e rápida deteção. Desde logo, o grau de confiança na utilização das TIC será necessariamente melhorado se for aumentado o nível de capacitação em matéria de proteção de dados e de literacia digital dos utilizadores do ciberespaço. Acreditamos, por isso, que a promoção da formação e da literacia digital irão contribuir para a rápida deteção e notificação de violações de dados pessoais.

---

[114] Cf. Veja-se o ciberataque através do vírus Notpetya de que a empresa AP Moller-Maersk foi alvo em 2017. Este foi considerado um dos maiores ciberataques alguma vez executados, pela extensão em número de países e pessoas afetadas, mas também pelos prejuízos com a reposição dos sistemas informáticos, lucros cessantes. Cf. GREENBERG, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", in WIRED, 22.08.2018, disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[115] Cf. estudo realizados pela Price WaterHouse Coopers «Information Security Breaches Survey 2017 – Redefining the security culture – a better way to protect your business». Segundo este estudo (cf. estudo p.5), a principal preocupação das empresas no que concerne a incidentes de segurança diz respeito à proteção da informação dos clientes.

A este respeito, os dados revelados nos Eurobarómetros 423[116] e 464a[117] indicam que os níveis de confiança dos cidadãos europeus na utilização do ciberespaço têm diminuído. Ora, cremos que estes dados resultam da falta de investimento na literacia e capacitação destes utilizadores, assim como da inexistência de selos de garantia ou certificações que atestem a conformidade dos softwares com os elevados padrões de proteção de dados pessoais que se esperam no tratamento de dados sensíveis.

Ainda neste âmbito, cumpre referir que os cidadãos revelam uma preocupação cada vez maior com a proteção dos seus dados pessoais e a sua privacidade. Todavia, como a aposta na educação para os temas tecnológicos ainda não foi verdadeiramente concretizada e a manutenção das parametrizações pré-definidas e previamente instaladas revela pouca pro-atividade dos utilizadores nestas matérias, parece reforçada a importância da formação para assegurar os princípios associados ao direito à proteção de dados.

Reitere-se que a aposta na educação, na literacia e no conhecimento constituem um investimento seguro que elevará o estádio de maturidade da sociedade para um patamar ainda não alcançado e que só auspicia os maiores augúrios na defesa dos direitos fundamentais, em especial, da proteção de dados pessoais (cf. art. 35.º da CRP) e da segurança (cf. art. 27.º da CRP), inclusivamente no ciberespaço.

1.10 Cooperação entre autoridades de controlo

Devido à maior digitalização dos serviços e à inelutável globalização, as violações de dados pessoais podem assumir um caráter transnacional, que não deve ser ignorado pelas autoridades de controlo competentes. Assim, para melhor responder aos desafios dessas violações, as autoridades de proteção de dados pessoais devem reforçar a comunicação e cooperação entre si.

No sentido de aferir o atual grau de interação entre várias autoridades de proteção de dados, foi realizado um exercício em 2015 entre o Centro Comum de Investigação (doravante CCI) da União Europeia em colaboração com a Direção-Geral da Justiça e dos Consumidores da Comissão Europeia e autoridades de proteção de dados de sete Estados-Membros (França, Alemanha, Grécia, Irlanda, Itália, Polónia e Espanha)[118]. Este foi o primeiro exercício pan-europeu de violações de dados pessoais

[116] Cf. Special Eurobarometer 423 – Cibersecurity, February 2015, disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf.

[117] Cf. Eurobarometer Europeans' attitudes towards cyber security, September 2017, disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171.

[118] Cf. MALATRAS, Apostolos, et al., «Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities», in Computer Law & Security Review, volume 33, Issue 4, August 2017, Elsevier, p. 458-469, disponível em: https://www.sciencedirect.com/science/article/pii/S0267364917300808.

e uma das suas principais constatações foi o entrave à cooperação devido a problemas de comunicação entre as diversas autoridades de proteção de dados.

Podemos extrair ilações seguras deste estudo, mas não podemos ignorar que a realidade fática em 2015 e 2018 é bastante diferente. O RGPD – com especial ênfase nos artigos 60.º e ss. –, a constituição do Comité Europeu para a Proteção de Dados (CEPD) em maio de 2018, a maior digitalização dos serviços, a sensibilização das autoridades de proteção de dados decorrente do próprio estudo, etc. permitiram aperfeiçoar as problemáticas comunicacionais. Não se pretende afirmar que foram ultrapassadas todas as questões, mas houve um progresso significativo da cooperação institucional entre as autoridades de proteção de dados.

Contudo, seria desejável a instituição de um procedimento uniforme que assegurasse a célere comunicação de violações de dados pessoais transnacionais entre as autoridades de proteção de dados. Atendendo à globalização de muitos serviços digitais e às vantagens inerentes a uma subdivisão de tarefas de investigação, bem como à partilha de informações que podem complementar o conhecimento detido por apenas uma entidade. A procura de sinergias é uma das chaves para a resposta concertada e eficaz face a violações de dados pessoais transnacionais. As autoridades de proteção de dados, os responsáveis pelo tratamento e os próprios cidadãos têm muito a ganhar com a comunicação e cooperação interinstitucional, designadamente no que respeita à partilha de informação e à melhor compreensão da complexidade e similitude de determinados ataques digitais.

A temática da cooperação entre autoridades de proteção de dados é inesgotável, quer no que respeita à competência da autoridade de controlo principal (cf. artigo 56.º do RGPD), à cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas (cf. artigo 60.º do RGPD) ou à assistência mútua (cf. artigo 61.º do RGDP). Muito poderia ser dito sobre os mecanismos de cooperação e assistência mútua, mas entendemos que estas questões extravasam o âmbito deste estudo. Contudo, é patente que os mecanismos de cooperação entre as autoridades de proteção de dados têm vindo a estreitar a sua relação e é louvável o empenho destas autoridades nesse sentido. Acreditamos que a cooperação entre as autoridades de controlo garantirá uma maior proteção dos dados dos titulares afetados numa violação de dados pessoais.

2. Procedimento para notificações de violações de dados pessoais

O responsável pelo tratamento de dados tem de comunicar as violações de dados pessoais à autoridade de controlo, sem demora injustificada, nas 72 horas seguintes à tomada de conhecimento das mesmas (cf. n.º 1 do artigo 33.º do RGPD). Durante este período é importante reunir os elementos descritos no n.º 3 do artigo 33.º e no n.º 3 do artigo 34.º do RGPD, consultando as pessoas mais habilitadas para efetuar todas as avaliações relevantes para as comunicações e notificações pertinentes.

Todavia, o RGPD não indica um esquema de comunicações que permita a recolha da informação obrigatória na notificação da autoridade de controlo e dos titulares dos dados afetados, que seja

eficiente e, simultaneamente, permita cumprir os prazos estabelecidos no próprio regulamento. Assim, pretendemos apresentar uma proposta de procedimento de comunicações internas e externas de violações de dados pessoais que possa ser utilizado pelos responsáveis pelo tratamento para facilitar o cumprimento das disposições constantes do RGPD.

Como nota preliminar, reiteramos que esta proposta não inclui as notificações de violações de dados pessoais com uma estrutura específica, como é o caso da obrigação de notificação imposta pelo artigo 4.º da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

De seguida, debruçar-nos-emos sobre as várias comunicações internas e externas após a deteção de um incidente que possa configurar uma violação de dados pessoais e atentaremos sobre uma proposta de procedimento de notificações de violações de dados, incluindo a sua demonstração prática.

2.1 Árvore de comunicação

Tomemos como referência a situação em que um colaborador do responsável pelo tratamento deteta uma suspeita de violação de dados pessoais. Neste cenário, em primeiro lugar, devem privilegiar-se as comunicações internas, não só para apurar a natureza e extensão da violação de dados pessoais, como também para conter e mitigar as suas consequências e informar as pessoas com capacidade de decisão. No entanto, como garantir que o fluxo de informação (relevante) chega, de facto, ao conhecimento das pessoas com poder de decisão dentro de uma organização?

Na verdade, a resposta a esta questão não se afigura simples. De facto, para que a informação seja transmitida dentro de uma organização de um modo fluído e célere, importa definir os canais e os interlocutores dessa transmissão da informação. A mera compilação de informação não garante a sua comunicação aos órgãos com capacidade de decisão. A informação sobre a violação de dados pessoais tem de ser primeiramente confirmada por pessoas habilitadas para esse efeito e deve ser redigida numa linguagem inteligível para a audiência a que se destina. Assim, uma comunicação efetiva exige que cada um dos interlocutores saiba quem é o destinatário da mensagem e utilize uma linguagem simples, intuitiva e acessível. Deste modo, a mensagem será transmitida o mais rapidamente possível aos órgãos dirigentes, para que possam tomar uma decisão informada.

Ora, o crescimento significativo de informação não reticular é um dos desafios que se coloca às organizações. Na sequência da recolha indiscriminada de uma miríade de dados de várias fontes e formatos – em grande medida motivada pelo baixo custo do armazenamento da informação e pela ideia de que quanto mais informação detivermos, melhores decisões tomaremos –, as organizações deixaram de ser criteriosas na seleção e sistematização da informação. Na verdade, as decisões dos dirigentes das organizações não podem atualmente assentar em conceitos predeterminados e estáticos, já que a realidade evolui constantemente e é cada vez mais imprevisível e exigente no tempo de

resposta. Por estas razões, a assimilação dinâmica da informação tem de exortar as organizações a tomarem decisões rapidamente com base em informação estruturada, sem prejuízo de a informação não estruturada – como, por exemplo, a que resulta de websites na Internet com baixa credibilidade – ser também considerada no processo de tomada de decisão, mas com menor peso. No que respeita às notificações de violações de dados pessoais, tanto interna como externamente, a informação tem de ser fundamentada e proveniente de uma fonte fidedigna para que as respostas sejam verdadeiramente adequadas.

Para tanto, importa que os responsáveis pelo tratamento adotem procedimentos para a facilitação da comunicação de informação estruturada entre os interlocutores chave dentro da organização. Antes de prosseguirmos este raciocínio, importa ter presente que as diferenças na dimensão de uma organização poderão ter reflexo no número de interlocutores antes da tomada de decisão. As organizações com uma escala maior podem ter mais intermediários, mas tal não põe em causa a cadeia de comunicação que iremos propor e descrever adiante. Nesse caso, poderão ser acrescentados mais nódulos até à chegada da informação aos órgãos com poder de decisão, sem prejuízo de ser sempre preferível reduzir o número de interlocutores ao mínimo necessário.

Assim, identificamos como principais atores no procedimento de notificações de violações de dados dentro de uma organização:

- A pessoa que deteta a violação de dados pessoais;
- O EPD;
- A equipa de TIC ou suporte informático;
- O departamento jurídico/advogados;
- Os órgãos com capacidade de decisão.

Como já vimos *supra*, o responsável pelo tratamento apenas tem de notificar a autoridade de controlo quando tenha tomado conhecimento de uma violação de dados pessoais. Essa tomada de conhecimento tem lugar quando o responsável pelo tratamento fica ciente, com um grau de certeza razoável, de que ocorreu um incidente que comprometeu a proteção de dados pessoais[119]. Todavia, é do interesse do responsável pelo tratamento tomar conhecimento dessa violação o mais celeremente possível, e não protelar esse momento, para que possa reagir atempadamente e circunscrever os seus possíveis efeitos adversos.

Nesse sentido, a sensibilização de todos os colaboradores para potenciais ameaças – como por exemplo manobras de engenharia social[120] –, que possam causar violações de dados pessoais, e para

[119] Cf. *EDPB Guidelines on Personal data breach notification under Regulation 2016/679*" do CEPD, de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827.

[120] Entende-se por engenharia social a exploração de vulnerabilidades humanas para a obtenção de informação de um modo indevido. Cf. GRANGER, Sarah, Social Engineering Fundamentals, Part I: Hacker Tactics, 2001. «Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust». Disponível em: https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics.

o seu rápido reporte é estratégica para o responsável pelo tratamento. Todos os colaboradores, sem exceção, devem estar alertados para eventuais riscos que ameacem a proteção de dados. Em suma, a pessoa que deteta a violação de dados pessoais está numa posição em que pode contribuir com informações sobre o contexto e sobre as circunstâncias desse incidente. Estando todos os colaboradores sensibilizados para a temática das violações de dados pessoais, a probabilidade da deteção de potenciais incidentes e a sua imediata comunicação ao EPD aumenta, por maioria de razão.

De facto, a verdadeira proteção de dados pessoais só pode ser obtida com a compreensão e envolvimento de todos, sem prejuízo de o responsável nomear pessoas com maiores responsabilidades e conhecimentos nesta matéria, designadamente um EPD. Como vimos, o EPD terá a capacidade para centralizar e analisar de um modo esclarecido as possíveis violações de dados pessoais que lhe sejam comunicadas. De igual modo, será o EPD que estará em melhor posição para reportar as violações de dados aos órgãos com capacidade de decisão[121], assim como para lhes prestar a orientação e as informações necessárias no sentido da notificação às autoridades de controlo. Na nossa opinião, o EPD é a figura chave que pode agilizar os processos de comunicação internos e externos, assim como as notificações de violações de dados pessoais nos termos do RGPD.

Complementarmente, o EPD poderá classificar a informação de acordo com o formulário de notificação de violações de dados pessoais disponibilizado pelas diversas autoridades de controlo. Será também o EPD que melhor conseguirá avaliar a informação e a gravidade do impacto da violação de dados, assim como poderá propor medidas concretas para cessar a violação e mitigar os seus efeitos adversos, conjuntamente com a equipa de suporte a violações de dados pessoais (se a mesma existir), a equipa de informática e o apoio jurídico. Por fim, terão de ser os órgãos com capacidade de decisão a assumir a decisão de notificação da violação de dados à autoridade de controlo e a resposta global a esse incidente.

No entanto, importa sublinhar que a obrigação de notificar a autoridade de controlo relativamente a violações de dados pessoais cabe ao responsável pelo tratamento, e não ao EPD. Por outras palavras, se o responsável pelo tratamento não pretender notificar uma violação de dados pessoais à autoridade de controlo a qual devesse ser notificada – consequentemente violando as disposições do RGPD –, não deverá o EPD fazê-lo à sua revelia. Porém, nesse caso, as consequências de não proceder às notificações de violações de dados quando deveria tê-lo feito terão de ser assumidas pelo responsável pelo tratamento, e não pelo EPD. A este respeito, aliás, veja-se o artigo 39.º do RGPD, o qual elenca entre as funções do EPD a cooperação com a autoridade de controlo, mas não o dever de notificar violações de dados pessoais. Esse dever compete ao responsável pelo tratamento, nos termos do n.º 1 do artigo 33.º do RGPD, pese embora o EPD seja o interlocutor ideal, já que é o ponto de contacto com as autoridades de controlo sobre questões relacionadas com o tratamento de dados (cf. alínea e) do n.º 1 do art. 39.º do RGPD).

[121] Cf. n.º 3 do artigo 38.º do RGPD in fine: O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.

Note-se que muitas comunicações de possíveis violações de dados terão de envolver a equipa de suporte a violações de dados pessoais, e/ou a equipa de informática /TIC, na medida em que o EPD poderá não ter toda a informação relevante sobre cada caso. Para tanto, a cooperação entre o EPD e estas equipas deve ser cultivada desde sempre, inclusivamente no desenho da política de proteção de dados. O mesmo se diga relativamente ao envolvimento do departamento jurídico/advogados do responsável pelo tratamento.

Ora, a linguagem e a apreciação de cada um destes atores pode ser diversa, contribuindo para falhas e preconceitos decorrentes de formações, sensibilidades e níveis de conhecimento diferentes. Para ultrapassar estas barreiras (linguística, conceptual, etc.), cumpre ter presente a contextualização, a clareza da linguagem, o concreto destinatário da mensagem que se pretende comunicar e a urgência na transmissão da informação. No caso de uma violação de dados, importa tornar a informação em ação, ou seja, que a comunicação interna de uma violação de dados pessoais desencadeie a verificação interna da necessidade (ou não) de notificar a autoridade de controlo.

Dependendo das repercussões de uma violação de dados pessoais, pode ser necessário o suporte específico de equipas de comunicação que saibam direcionar melhor as mensagens para restabelecer a confiança no responsável pelo tratamento e a sua reputação. Nesse sentido, pode ser equacionada a intervenção de uma equipa especializada em comunicação em cooperação com o EPD.

No entanto, as comunicações da violação de dados pessoais não podem cingir-se à organização que a sofre. É igualmente necessário comunicar essa violação a um outro conjunto de atores do tratamento de dados pessoais externos à organização, mas que direta ou indiretamente podem ser afetados pela mesma. Numa perspetiva interinstitucional, a deteção de uma violação de dados e a sua comunicação a outros atores do mesmo tratamento de dados pode ser muito relevante para a sua análise, cessação e mitigação de eventuais efeitos adversos. Inclusivamente, podem ser estes atores fora da organização os primeiros a detetar a violação de dados e a comunicá-la ao responsável pelo tratamento.

Assim, ainda antes de notificar as autoridades de controlo com competência e, se aplicável os OPC e os próprios titulares dos dados afetados, temos igualmente de atender às linhas de comunicação de violações de dados pessoais entre os vários atores de um tratamento de dados pessoais externos à estrutura do responsável pelo tratamento, ou seja:

- Responsáveis conjuntos;
- Subcontratantes;
- Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na EU (art. 27.º RGPD).

Portanto, deve ser implementado um plano estratégico de comunicação de violações de dados entre o responsável pelo tratamento, responsáveis conjuntos, subcontratante e seus representantes para definir e melhor direcionar as linhas de comunicação. Recordemos que as partes dispõem de liberdade contratual (cf. artigo 405.º do Código Civil) para definirem um sistema de comunicações, já que o RGPD

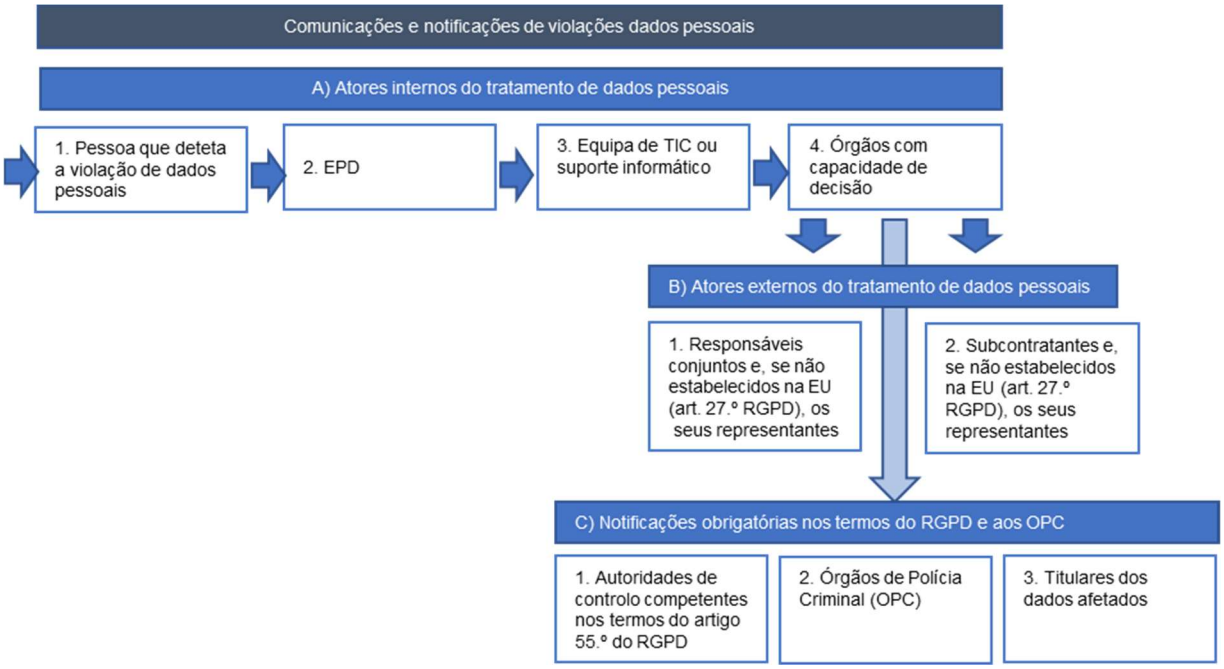
não determina uma cadeia de notificações entre responsáveis pelo tratamento, subcontratantes e seus representantes. Nesse sentido, as partes são livres de fixar o conteúdo dos contratos que celebram, desde que não violem o disposto na lei[122]. Portanto, nada impede que as partes acordem uma cadeia de comunicação entre si no que respeita às violações de dados pessoais de que tomem conhecimento. Assim, a partir desse momento ficam vinculadas a essa nova obrigação de comunicarem numa determinada ordem e forma as violações de dados pessoais que envolvam as demais partes no contrato e cheguem ao seu conhecimento.

Entendemos que a comunicação deve ser feita simultaneamente aos responsáveis pelo tratamento e aos seus representantes, quando os primeiros não estejam estabelecidos na UE (cf. art. 27.º do RGPD). O mesmo se diga relativamente aos subcontratantes e aos seus representantes quando não estabelecidos na EU (cf. art. 27.º RGPD). Uma vez que o RGPD prevê esta figura dos representantes – a qual já se encontrava prevista no anterior quadro legal na Diretiva 95/46/CE –, acreditamos que a proximidade geográfica da sua localização na UE pode beneficiar a implementação de medidas de segurança necessárias e a comunicação com as autoridades de controlo. Acresce que não antevemos nenhum prejuízo no envolvimento desta figura, tanto mais que o n.º 4 do artigo 27.º do RGPD refere que o representante é mandatado para ser contactado em complemento ou em substituição do responsável pelo tratamento ou do subcontratante, em especial por autoridades de controlo e por titulares – mas não exclusivamente –, relativamente a todas as questões relacionadas com o tratamento.

Sabendo que o objetivo destas comunicações internas consiste na deteção, contenção, investigação, mitigação e recuperação face a uma violação de dados pessoais, bem como na sua notificação às autoridades de controlo e aos titulares dos dados afetados – nos termos dos artigos 33.º e 34.º do RGPD –, a linha de comunicações entre os diversos intervenientes deve ser o mais direta possível.

Figura 4 – Árvore de comunicações e notificações de violações de dados pessoais entre os diversos atores do tratamento de dados pessoais

[122] Cf. RIBEIRO DE FARIA, Jorge, Direito das Obrigações, Vol. I, Almedina, 2003.



Legenda: Cadeia de comunicações e notificações de violações de dados pessoais, quando detetadas pelo responsável pelo tratamento, envolvendo os diversos atores no ecossistema de um tratamento de dados pessoais.

Assim, tal como descrito na tabela *supra*, entendemos que as comunicações internas devem preceder as comunicações externas, as quais devem ter lugar antes das notificações à autoridade de controlo e aos titulares dos dados, nos termos do RGPD.

Ora, o esquema de comunicações internas e externas *supra* descrito parte do princípio de que a pessoa que deteta a violação de dados pessoais integra a estrutura interna do responsável pelo tratamento. Todavia, pode suceder que a violação de dados pessoais seja detetada por um interveniente externo à estrutura do responsável pelo tratamento. Neste cenário, tem de ser criada uma outra árvore de comunicações para que o responsável pelo tratamento tome conhecimento da violação de dados pessoais e, nessa qualidade, execute ou faça executar as operações necessárias para cessar e mitigar os efeitos dessa violação, concomitantemente documentando todas as ações, para que possa devidamente notificar a autoridade de controlo.

Vejamos, então, a hipótese em que uma possível violação de dados pessoais é detetada por um ator externo ao responsável pelo tratamento. Neste caso, a suspeita ou uma efetiva violação de dados pessoais deve, o mais prontamente possível, ser trazida ao conhecimento do EPD do responsável pelo tratamento, para que este possa centralizar todas as comunicações com os demais atores, e inclusivamente para principiar a avaliação inicial em nome do responsável pelo tratamento.

Com vista a ilustrar quem deve proceder a estas comunicações, atentemos na proposta de comunicações constante da tabela *infra*, que esquematicamente detalha as possíveis comunicações com atores externos à estrutura do responsável pelo tratamento, mas com envolvimento no tratamento de dados pessoais.

Figura 5 – Árvore de comunicações de violações de dados pessoais entre os diversos atores do tratamento de dados pessoais

		Comunicação da violação de dados pessoais aos						
		A) Atores internos do tratamento de dados pessoais			B) Atores externos do tratamento de dados pessoais			
		1. EPD	2. Equipa de TIC ou suporte informático	3. Órgãos com capacidade de decisão	4.1 Responsável(eis) pelo tratamento	4.2 Representante do responsável pelo tratamento	5.1 Subcontratante(s)	5.2. Representante do subcontratante
Violação de dados pessoais detetada pelo	Hipótese A) Responsável pelo tratamento	√	√	√	√ (apenas aplicável nos casos de responsabilidade conjunta - cf. art. 26.º do RGPD)	√ (apenas aplicável nos casos de responsabilidade conjunta - cf. art. 26.º do RGPD)	√	√
	Hipótese B) Representante do responsável pelo tratamento	√	√	√	√, EPD do responsável pelo tratamento	n/a	√, se mandatado para o efeito pelo responsável pelo tratamento	√, se mandatado para o efeito pelo responsável pelo tratamento
	Hipótese C) Subcontratante	√	√	√	√, ao EPD do responsável pelo tratamento	√	√	√
	Hipótese D) Representante do subcontratante	√	√	√	√, ao EPD do responsável pelo tratamento	√	√	n/a
	Hipótese E) Outros (ex. cliente, etc.)	n/a	n/a	n/a	√, mas não é obrigatória	n/a	n/a	n/a

n/a: não aplicável
√ : comunicar

Legenda: Cadeia de comunicações e notificações de violações de dados pessoais, quando não detetadas pelo responsável pelo tratamento, envolvendo os diversos atores no ecossistema de um tratamento de dados pessoais

Com o esquema proposto neste estudo não se pretende duplicar as comunicações entre os diferentes atores no tratamento de dados pessoais. Pelo contrário, pretendemos criar um sistema que evite a duplicação de comunicações, ou dependa de cadeias paralelas de comunicações, e garanta um fluxo efetivo e atempado da informação entre os atores que devem conhecer da violação de dados pessoais.

Antes de prosseguirmos com esta análise, cumpre ressalvar que, por vezes, são os subcontratantes quem possui os meios para cessar e/ou mitigar os efeitos adversos de uma violação de dados pessoais, e não o responsável pelo tratamento. Ora, daqui se conclui que a árvore de comunicações entre responsável pelo tratamento, subcontratantes e seus representantes deverá ser vista casuisticamente.

Em qualquer dos casos – ou seja, no caso de a violação de dados pessoais ter sido detetada pelo responsável pelo tratamento ou por outro ator do ecossistema do tratamento de dados pessoais –, tomamos a liberdade de propor uma solução que poderá ser eficaz para a maior parte das hipóteses, dado que o responsável pelo tratamento deve ser sempre informado das medidas aplicadas pelos subcontratantes, não só para poder instruir o subcontratante no que respeita ao tratamento de dados pessoais na sequência da violação de dados, como também para notificar a autoridade de controlo, nos termos do RGPD.

A este respeito, recordemos que o subcontratante apenas deve tratar os dados pessoais mediante as instruções documentadas do responsável pelo tratamento (cf. alínea a) do n.º 3 do art. 28.º do RGPD) e deve prestar assistência ao responsável pelo tratamento para que este possa cumprir as obrigações previstas nos artigos 33.º e 34.º do RGPD (cf. alínea f) do n.º 3 do art. 28.º do RGPD). Portanto, qualquer suspeita séria de uma violação de dados pessoais por parte de um dos atores do tratamento de dados pessoais deve ser prontamente comunicada e verificada internamente antes de ser comunicada ao responsável pelo tratamento.

Lembremos também que o prazo de 72 horas para a notificação da violação de dados pessoais pelo responsável pelo tratamento à autoridade de controlo apenas se inicia a partir do momento em que este tome conhecimento daquela violação. Logo, caso o subcontratante ou outro ator detetem uma violação de dados pessoais, devem primeiro acionar o plano de comunicações internas dentro da sua organização, nomeadamente informando o seu próprio EPD (caso tenha sido designado), que tomará as medidas que entender necessárias junto da equipa de TIC e dos órgãos com poder de decisão. Como vimos, o dever de notificar a autoridade de controlo é uma obrigação do responsável pelo tratamento[123]. Portanto, o prazo para a notificação da autoridade de controlo apenas inicia na data da efetiva tomada de conhecimento da violação de dados pessoais pelo responsável pelo tratamento, não interferindo as aferições efetuadas pelo EPD do subcontratante ou de outro ator no tratamento de dados anteriormente à comunicação da violação ao responsável pelo tratamento no início da contagem do

[123] Uma vez que o artigo 27.º do RGPD prevê expressamente a obrigação de os responsáveis pelo tratamento não estabelecidos na UE designarem um representante, entendemos que a obrigação de notificação de violações de dados pessoais à autoridade de controlo poderia ser delegada neste outro ator. Todavia, como o RGPD é omisso quanto a esta possibilidade, seguimos o argumento literal de apenas o responsável pelo tratamento exercer diretamente esta obrigação de notificação.

mesmo. Deste modo, quando a violação de dados pessoais for comunicada pelos demais atores ao responsável – momento da tomada de conhecimento efetiva, a partir da qual inicia a contagem de 72 horas para a notificação da violação de dados à autoridade de controlo – este terá as informações constantes da aferição inicial efetuada pelo EPD da organização que comunica a violação, e poderá iniciar a sua própria análise (avaliação inicial) e tomar as medidas necessárias, quer junto do subcontratante, quer de outros atores da arena de proteção de dados.

De ressalvar ainda que nos casos de responsabilidade conjunta, o prazo para a notificação da autoridade de controlo tem início na data em que qualquer um dos responsáveis conjuntos tome conhecimento efetivo da violação de dados pessoais, independentemente de comunicar essa violação aos demais responsáveis pelo tratamento. Por essa razão, os responsáveis pelo tratamento / responsáveis conjuntos (e os seus representantes quando os primeiros não estejam estabelecidos na UE) devem ser notificados em primeiro lugar após a aferição interna por um outro ator envolvido no tratamento de dados, na medida em que têm responsabilidade pelo cumprimento do RGPD. Naturalmente que o grau de responsabilidade poderá variar entre os diversos responsáveis conjuntos, mas os titulares dos dados e as autoridades de controlo podem intentar ações judiciais diretamente contra um dos responsáveis conjuntos, sem prejuízo de este exigir o direito de regresso junto dos demais responsáveis – como vimos no capítulo II.4 deste estudo. Por essa razão, e porque os responsáveis conjuntos determinam as finalidades e os meios do tratamento de dados pessoais, devem ser os primeiros na linha de notificações externas. Porque os responsáveis pelo tratamento não estabelecidos na UE têm de designar por escrito um representante na EU (cf. artigo 27.º do RGPD), devem estes atores ser simultaneamente notificados com os responsáveis pelo tratamento pelo ator que deteta a violação de dados.

Sumariando a nossa proposta de cadeia de comunicações, logo que seja identificada uma violação de dados pessoais, deve a mesma ser comunicada ao EPD da organização que a deteta, o qual envidará os esforços necessários junto da equipa de TIC para apurar se se trata de uma violação de dados pessoais – documentando a informação relevante – e informar os órgãos com poder de decisão. Nessa sequência, os órgãos com poder de decisão poderão adotar medidas de cessação, contenção, mitigação e reparação dos efeitos adversos da violação de dados pessoais, bem como proceder à comunicação dessa violação ao responsável pelo tratamento. Uma vez transmitida a comunicação ao responsável pelo tratamento, de preferência diretamente ao EPD, deve este iniciar a sua própria análise com base nos elementos transmitidos e noutros que entender pertinentes. Seguidamente deve a equipa de TIC do responsável pelo tratamento ser envolvida para a avaliação inicial, a qual será reportada aos órgãos com poder de decisão do responsável pelo tratamento. No fundo, a partir do momento em que a cadeia de informação chega ao EPD do responsável pelo tratamento aplica-se a cadeia de comunicações previstas *supra* para as violações de dados pessoais detetadas por uma pessoa dentro da estrutura do responsável pelo tratamento.

Por fim, e como já várias vezes sublinhado neste trabalho, importa proceder às notificações obrigatórias nos termos do RGPD. Consequentemente, após as devidas comunicações internas e externas, cumpre proceder – se aplicável – às notificações:

- Às autoridades de controlo competentes nos termos do artigo 55.º do RGPD;
- Aos OPC;
- Aos titulares dos dados afetados.

Estas notificações constituem uma obrigação do responsável pelo tratamento e não devem ser efetuadas por outros atores externos, como o subcontratante ou representante do subcontratante. Na verdade, seguindo a boa prática de designar um EPD, deverá ser este a efetuar a notificação à autoridade de controlo em nome do responsável pelo tratamento, enquanto pessoa mais habilitada para o efeito.

Relativamente à forma de todas as comunicações acima descritas, entendemos que devem ser efetuadas por escrito (por exemplo, por email, relatório, etc.) para facilitar a documentação e prova, sem prejuízo da sua confirmação por outro meio mais expedito, como uma reunião ou telefonema.

Por último, caso seja necessária a notificação à autoridade de controlo com competência em matéria de proteção de dados – prevista no artigo 33.º do RGPD – a intervenção dos OPC e a notificação aos titulares dos dados afetados, – nos termos do artigo 34.º do RGPD – o responsável pelo tratamento já reuniu um conjunto de elementos que lhe permitem aferir essa obrigação. Ademais, esses mesmos elementos possibilitarão a colocação em prática de um plano de reposta que reduza o impacto negativo da violação de dados pessoais.

Todavia, relembramos que o RGPD prevê a possibilidade de não ter sida reunida toda a informação necessária para a notificação de uma violação de dados pessoais nas 72 horas seguintes à tomada de conhecimento pelo responsável pelo tratamento, nos termos do seu artigo 33.º. Em especial nos casos de violações de dados complexas ou de grande escala, acreditamos que pode não ser possível cumprir o prazo de 72 horas para a recolha de todos os elementos constantes do n.º 3 do artigo 33.º do RGPD. Nesses casos, o responsável pelo tratamento deve proceder a uma notificação de acordo com os elementos de que dispõe dentro daquele prazo, justificando a impossibilidade de facultar determinados elementos.

2.2 Proposta de procedimento para notificações de violações de dados pessoais

Atendendo às boas práticas enunciadas no início deste capítulo e aos atores que devem ser envolvidos nas comunicações internas e externas, assim como às notificações de violações de dados pessoais nos termos do RGPD, vejamos agora uma proposta concreta de um procedimento para notificações de violações de dados pessoais que engloba esquematicamente as comunicações entre os diversos atores do ecossistema de proteção de dados. Nesta proposta contemplamos as medidas prévias mínimas que permitem a rápida deteção da violação de dados pessoais que desencadeia as

comunicações que devem ser operadas entre os diversos interlocutores, incluindo os atores específicos que devem proceder às comunicações/notificações e os seus prazos.

Esta proposta sumaria a informação supra descrita neste trabalho. Segundo a nossa proposta, a forma mais eficaz de garantir que as comunicações internas e externas circulam fluidamente por quem delas deva tomar conhecimento privilegia o papel do EPD e coloca em evidência a sua importância no tratamento de dados pessoais, em especial, nas situações de violações de dados pessoais.

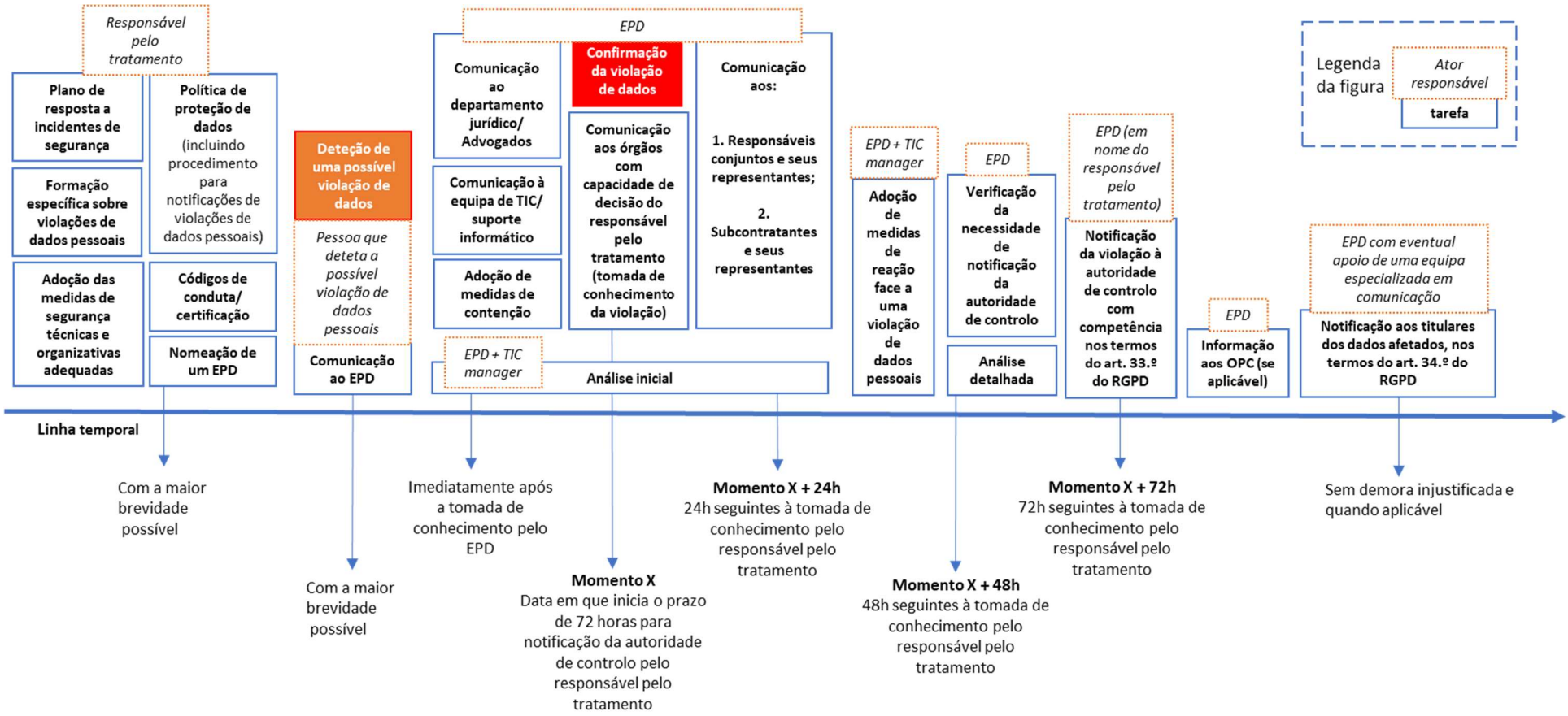
Recordemos que o EPD do responsável pelo tratamento é o ator que tem conhecimento especializado em matéria de proteção de dados pessoais, assim como sobre os tratamentos de dados pessoais operados pelo responsável pelo tratamento. Ademais, encontra-se numa posição em que reporta diretamente à direção ao mais alto nível (cf. n.º 3 do artigo 38.º in fine do RGPD).

Neste contexto, o EPD pode e deve ser a figura principal na gestão de uma violação de dados pessoais. É o EPD que – sozinho ou conjuntamente com apoio de especialistas informáticos – confirma a ocorrência de uma violação de dados pessoais, que a reporta diretamente aos órgãos de direção do responsável pelo tratamento ao mais alto nível e que propõe medidas reativas. A análise bifásica da violação de dados deve ser efetuada pelo EPD, sem prejuízo de suporte específico em matérias jurídicas e/ou informáticas. O EPD é igualmente quem constitui o contacto privilegiado com a autoridade de controlo, mas também com os titulares dos dados (cf. n.º 4 do artigo 38.º e alínea e) do n.º 1 do artigo 39.º do RGPD).

Por essa razão, o responsável pelo tratamento deve facultar ao EPD os recursos necessários (humanos, financeiros e de acesso transparente aos dados pessoais e às operações de tratamentos de dados) para o cabal desempenho das suas funções e para a sua contínua atualização de conhecimentos (cf. n.º 2 do artigo 38.º do RGPD).

Atentemos, então, na figura *infra* que esquematicamente sumaria a nossa proposta de notificações de violações de dados pessoais entre os diversos atores num tratamento de dados pessoais.

Figura 6 – Proposta de procedimento de comunicações/notificações de violações de dados pessoais



Legenda: Proposta de procedimento de notificações de violações de dados pessoais contemplando medidas prévias mínimas que permitem a rápida deteção da violação de dados pessoais que desencadeia a cadeia de comunicações, as comunicações que devem ser operadas entre os diversos interlocutores, os atores que devem proceder às comunicações/notificações e os seus prazos.

2.3 Demonstração da validade e viabilidade da proposta

Com vista a comprovar a validade e eficácia do procedimento para notificações de violações de dados pessoais *supra* descrito, solicitámos a uma empresa de recrutamento portuguesa (Vitae Professionals, Lda.) a sua validação.

Com vista a melhor contextualizar a empresa, elencamos *infra* alguns elementos pertinentes do ponto de vista do tratamento de dados pessoais.

Figura 7 – Perfil da Empresa Vitae Professionals

Área de atividade	Empresa de recrutamento
N.º de trabalhadores	8
Categorias de dados pessoais tratados	Perfil socio-demográfico, dados de contacto, *curricula vitae* dos recrutandos, testes de aferição de conhecimento, dados de saúde, certificado de registo criminal, fotografias, IBAN.
Categorias especiais de dados pessoais	Sim
N.º de trabalhadores que participou na formação sobre proteção de dados e notificações de violações de dados pessoais	8
Nomeação de um Encarregado de Proteção de Dados	Sim
Certificação de qualidade	Sim

Legenda: Tabela informativa com dados relevantes para o tratamento de dados pessoais relativa à empresa participante no caso de estudo.

Assim, aplicámos um questionário (cf. Anexo 1 deste estudo) aos colaboradores desta empresa para avaliar o seu grau de conhecimentos sobre a melhor forma de agir perante um possível incidente implicando uma violação de dados pessoais ainda antes da adoção de uma política de proteção de dados, contemplando um procedimento de comunicações internas e externas.

Constatámos um bom nível de proatividade dos colaboradores desta empresa na comunicação da informação (87,5%), os quais na sua maioria e ainda antes das formação indicaram comunicar em primeiro lugar uma possível violação de dados pessoais ao EPD.

De seguida, a Vitae Professionals adotou um procedimento para notificação de violações de dados pessoais nos termos *supra* descritos neste capítulo, seguindo o esquema constante da figura 5. Foi ainda ministrada uma formação específica sobre violações de dados pessoais a todos os colaboradores e à EPD desta empresa, e aplicado novamente o mesmo questionário aos seus colaboradores para avaliar o impacto da formação e do procedimento na sua conduta perante um possível incidente implicando uma violação de dados pessoais.

Na formação foi explicado o conceito de dado pessoal, de violação de dados pessoais, de EPD, entre outros conceitos relevantes. Foi igualmente feita uma sensibilização para manobras de engenharia social e explicadas quais as possíveis implicações de violações de dados pessoais. Por fim, foi indicado qual o procedimento a adotar em caso de uma suspeita de violação de dados pessoais.

De acordo com o segundo questionário, a totalidade dos colaboradores da empresa neste estudo de caso identificou corretamente uma suspeita de violação de dados pessoais e indicou que comunicariam imediatamente essa suspeita à EPD.

A EPD da Vitae Professionals reconheceu que o impacto da formação foi muito significativo na sensibilização de todos os colaboradores e que estes se sentem mais seguros com os procedimentos a adotar. A própria EPD referiu que estava mais confiante com o procedimento de notificações sugerido neste trabalho e adotado pela empresa. Sendo a própria sujeita a uma pequena simulação de uma violação de dados pessoais, foi exequível o contacto de todo o organigrama de pessoas que a EPD deveria contactar nas 24 horas seguintes à violação de dados pessoais fictícia.

Relativamente aos subcontratados, a Vitae Professionals, Lda. adotou igualmente o mesmo procedimento de comunicações de violações de dados pessoais, estando agora todos cientes de qual a cadeia de comunicações a adotar. Adicionalmente, a Vitae Professionals adotou boas práticas em matéria de medidas de segurança técnicas.

Assim, podemos dizer que o procedimento proposto é um mecanismo que auxilia o responsável pelo tratamento a cumprir a obrigação de notificação das violações de dados pessoais à autoridade de controlo e aos titulares dos dados afetados, nos termos do RGPD. Daqui se conclui que a proposta apresentada não só facilita o cumprimento do disposto no RGPD, como promove a proteção de dados pessoais em geral.

Conclusões

1. O direito à proteção de dados é um direito fundamental consagrado no n.º 1 do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, no n.º 1 do artigo 16.º do Tratado sobre o Funcionamento da União Europeia, nos artigos 26.º e 35.º da Constituição da República Portuguesa, pelo que foi reforçado juridicamente com o RGPD.

2. O progresso tecnológico e a globalização permitem que as violações de dados pessoais adquiram uma grande escala e impacto num curto espaço de tempo, justificando a preocupação com esta temática por parte do legislador nacional e europeu, dos responsáveis pelo tratamento e da sociedade em geral.

3. O possível impacto de violações à proteção de dados pessoais nos direitos e liberdades das pessoas singulares justificou a atenção do legislador europeu que prescreve no RGPD a obrigação da sua notificação à autoridade de controlo competente e aos titulares dos dados afetados – destes últimos quando haja um risco elevado para os seus direitos e liberdades.

4. A este respeito, o RGPD veio alterar o paradigma da proteção de dados pessoais, sublinhando a responsabilidade dos responsáveis pelo tratamento e a transparência dos tratamentos de dados. Nessa medida, comporta entre as suas novidades a obrigatoriedade de todos os responsáveis pelo tratamento notificarem as violações de dados pessoais de que sejam alvo à autoridade de controlo e aos titulares dos dados afetados, nos termos dos artigos 33.º e 34.º do RGPD.

5. Através da análise crítica dos requisitos e para facilitar as notificações de violações de dados pessoais nos termos do RGPD, consideramos necessária a definição de orientações, boas práticas e a facilitação de cadeias de comunicação entre os diversos interlocutores.

6. Para cumprir os prazos, assim como recolher a informação necessária para a devida notificação das violações de dados às autoridades de controlo e aos titulares dos dados afetados nos termos do RGPD, entendemos que o responsável pelo tratamento de dados pessoais deve adotar não só as medidas de segurança adequadas – quer preventivas quer reativas e contemplando uma possível violação de dados pessoais –, como também boas práticas.

7. Entre estas boas práticas recomendamos a planificação e adoção de uma política de proteção de dados, a implementação de um plano de resposta a incidentes de segurança, a adoção de medidas de segurança técnicas e organizativas adequadas para cada tratamento de dados pessoais, a adoção de códigos de conduta ou certificações em matéria de proteção de dados, a avaliação bifásica do impacto da violação de dados pessoais após a sua tomada de conhecimento, investigação e documentação de todos os procedimentos, aposta em recursos humanos e materiais para a deteção e reparação de violações de dados pessoais, incluindo a

nomeação de um EPD e a definição de uma equipa de suporte a violações de dados pessoais, a formação/sensibilização de todos os colaboradores e a cooperação entre autoridades de controlo nas violações transnacionais.

8. Todavia, estas boas práticas não bastam para a efetiva recolha da informação necessária na notificação de violações de dados pessoais dentro dos prazos estabelecidos no RGPD. Assim, delineamos uma proposta de procedimento para responder aos desafios de uma notificação de violações de dados pessoais às autoridades de controlo e titulares dos dados afetados, nos termos do RGPD.

9. Apesar de o RGPD não o prescrever expressamente, entendemos que a adoção de um procedimento de comunicações/notificações de violações de dados pessoais pelo responsável pelo tratamento contribui para a observância dos requisitos relativos a esta temática.

10. A iniludível primazia do EPD nesta proposta de procedimento de comunicações/notificações de violações de dados pessoais vem demonstrar a relevância deste ator no ecossistema de um tratamento de dados pessoais, enquanto especialista na matéria, avaliador abalizado do risco para os titulares dos dados e contacto privilegiado com os vários atores em causa.

11. No nosso ponto de vista, esta proposta promove os direitos fundamentais dos titulares dos dados, evidencia a preocupação do responsável pelo tratamento no que respeita ao cumprimento do RGPD e eleva a proteção de dados de um modo geral.

12. Demostrámos a eficácia desta proposta numa PME portuguesa, através da aferição do nível de conhecimento dos colaboradores antes e depois de uma formação específica sobre os comportamentos a adotar perante violações de dados pessoais, da adoção da nossa proposta de procedimento de comunicações e notificações internas e externas relativamente a essas violações e do teste da sua exequibilidade em tempo real.

13. Acreditamos que este procedimento pode e deve ser replicado noutras PME e organizações que sejam responsáveis pelo tratamento de dados pessoais.

Bibliografia

ANDRESS, Jason, The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice, 2.ª edição, Elsevier/Syngress, 2014.

ANTUNES VARELA, Direito da Sociedade de Informação (coord.: José de Oliveira Ascensão), vols. I-X, Coimbra: Coimbra Editora, 1999/2012.

BARNARD-WILLS, D. et al., Data protection authority perspectives on the impact of data protection reform on cooperation in the EU, Computer Law & Security Review, volume 34, Issue 4, 2016, p. 587-598.

BOYCE, Joseph, JENNINGS, Dan, Information Assurance – a practical guide: Managing Organizational IT securit risks, Butterworth Heinemann, 2002.

CABRAL BARRETO, Irene, Convenção Europeia dos Direitos do Homem, 5.ª Edição, Almedina, 2015.

CANOTILHO, José Gomes, Direito Constitucional e Teoria da Constituição, 5.ª Edição, Almedina, 2002.

CARRIE WONG, Julia, «Uber concealed massive hack that exposed data of 57m users and drivers», in The Guardian 22.11.2017, disponível em https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

CASEY, Eoghan, Handbook of Digital Forensics and Investigation, Academic Press, 2010.

CASEY, Eoghan, Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers, and the Internet, Academic Press, 2011.

CASTELLS, Manuel, A Era da Informação: Economia, Sociedade e Cultura, Volume I, A sociedade em rede, Fundação Calouste Gulbenkian, 2011.

Computer Security Incident Handling Guide do National Institute of Standards and Technology/U.S. Department of Commerce, disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

DIFFIE, Whitefield e HELLMAN, Martin, «New Directions in Cryptography», IEEE Transaction on Information Theory, vol. IT-22, n.º 6, novembro 1976, disponível em: https://www-ee.stanford.edu/~hellman/publications/24.pdf.

ESKENS, S., HELBERGER, N. and MOELLER, J., «Challenged by news personalisation: five perspectives on the right to receive information», in Journal of Media Law, 9(2), 2017, pp.259-284.

FAISAL, M.A., AUNG Z., WILLIAMS, J.R., SANCHEZ, A., Securing advanced metering infrastructure using intrusion detection system with data stream mining, 2012 Pacific AsiaWorkshop on Intelligence and Security Informatics (PAISI 2012); 2012. pp. 96–111.

FARINHO, Domingos Soares, Intimidade da Vida Privada e Media no Ciberespaço, Almedina, 2006.

FU, Zhiwei, «Manage what is known and what is unknown: a roadmap to management enterprise fraud risk», in ISACA Journal, Vol. 5, 2014.

FUENTE ANUNCIBAY, Raquel, «ICTs and Teenage Students. Problematic Usage or Dependence» in Procedia - Social and Behavioral Sciences, Volume 237, 21 February 2017, Pages 230-236.

GALLOWAY, Scott, The four: the hidden DNA of Amazon, Apple, Facebook and Google, Random House Large Print, 2017.

GÓMEZ URGELLÉS, Joan-Vincenç, «Matemáticos, Espiões e Piratas Informáticos, Codificação e Criptografia», Edição Especial National Geographic, 2016.

GOODMAN, B. and FLAXMAN, S., European Union regulations on algorithmic decision-making and a "right to explanation". 3rd ed., New York: University of Oxford, 2016, disponível em: https://arxiv.org/pdf/1606.08813.pdf.

GRANGER, Sarah, Social Engineering Fundamentals, Part I: Hacker Tactics, 2001. Disponível em: https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics.

GREENBERG, Andy, «The Untold Story of NotPetya, the Most Devastating Cyberattack in History», in WIRED, 22.08.2018, disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

GUTWIRTH, S. and de HERT, P., «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power», in Privacy and the criminal law. Antwerp/ Oxford: Intersentia, 2006, pp.61-104.

HERN, Alex, WATERSON, Jim, «Sites block users, shut down activities and flood inboxes as GDPR rules loom», in The Guardian, 24.05.2018, disponível em: https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect.

HIJMANS, H., Understanding the role of cooperation mechanisms of DPAs: towards a layered model of horizontal cooperation between DPAs, a structured network of DPAs and a European DPA, in The European Union as a guardian of internet privacy, Springer International Publishing, 2016, p. 389-448.

HITCHCOCK, Ben, LE-KHAC, Nhien-An, SCANLON, Mark, Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists, in Digital Investigation 16, Elsevier, 2016.

INFORMATION COMMISSIONER'S OFFICE, Investigation into the use of data analytics in political campaigns – investigation update, 2018, disponível em: https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf.

ISAZA G, CASTILLO A, LÓPEZ M, CASTILLO L. Towards ontology-based intelligent model for intrusion detection and prevention. Advances in Soft Computing, Springer, 2009.

JIMÉNEZ, Luis, «Evolución histórica y conceptual del derecho a la vida privada», in Revista de Los Tribunales Agrarios, Segunda Época, n.º 42, año IV, Mayo-Agosto de 2007.

KARYDA et. al., Breach Notification: Issues and Challenges for Security Management, Tenth Mediterranean Conference on Information Systems (MCIS), Paphos, Cyprus, September 2016, disponível em: https://www.researchgate.net/profile/Maria_Karyda/publication/309414062_DATA_BREACH_NOTIFICATION_ISSUES_AND_CHALLENGES_FOR_SECURITY_MANAGEMENT/links/580f4b4608aef2ef97afc0b2/DATA-BREACH-NOTIFICATION-ISSUES-AND-CHALLENGES-FOR-SECURITY-MANAGEMENT.pdf.

KASPER, Agnes, LAURITS, Eneli, «Challenges in Collecting Digital Evidence: A Legal Perspective», in The Future of Law and eTechnologies, Springer, 2016, p. 195-233.

KASSIN, Saul M., DROR, Itiel E., KUKUCKA, Jeff, Target article: The forensic confirmation bias: Problems, perspectives, and proposed solutions, in Journal of Applied Research in Memory and Cognition, 2013.

KELLY, Martin et al., «Data Privacy: Effects on Customer and Firm Performance», in Journal of Marketing, Sage Journals, Volume: 81 issue: 1, page(s): 36-58 October 8, 2018, disponível em http://journals.sagepub.com/doi/10.1509/jm.15.0497.

LAMBERT, Paul, The Data Protection Officer – Profession, Rules and Role, CRC Press, 2016.

LIEBER, Ron, «How to protect yourself after the Equifax Breach», in The New York Times, 2017 (atualizado em 16.10.2017), disponível em: https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html.

MALATRAS, Apostolos, et al., Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities, Computer Law & Security Review, volume 33, Issue 4, August 2017, p. 458-469.

MENEZES LEITÃO, Luís Manuel Teles, Direito das Obrigações – Volume I: Introdução da Constituição das Obrigações, 15ª Edição, Almedina Editora, 2018.

MIRANDA, Jorge, Manual de Direito Constitucional, 3.ª Edição, Tomo IV Coimbra Editora, 2000.

MOCHMANN, Ekkehard e MÜLLER, Paul J., Data Protection and Social Science Research: Perspectives from Ten Countries, Campus-Verlag, 1979.

NIETO, Ana, ROMAN, Rodrigo, LOPEZ, Javier, «Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices», in Network Forensics and Surveillance for Emerging Networks, IEEE Network, November/December, 2016.

PAAR, Christof, PELZL Jan, Understanding cryptography: a textbook for students and practicioners, Springer, 2010.

PALMA, Maria Fernanda, «Tutela da vida privada e processo penal», JC 10 (2006), p. 3-12.

PATEL, Ahmed, ALHUSSIAN Hitham, PEDERSEN Jens et al., «A nifty collaborative intrusion detection and prevention architecture for Smart Grid Ecosystems», in Computers and Security 64 (2017), Elsevier, p.92-109.

PINTO, Frederico Lacerda Costa e BELEZA, Teresa Pizarro, Prova Criminal e Direito de Defesa – Estudos sobre a teoria da prova e garantias de defesa em processo Penal, Almedina, 2016.

RAMOS, Armando Dias, A Prova Digital em Processo Penal: o Correio Eletrónico, 2.ª Edição, Chiado Editora, 2014.

RASSIN, Eric, «Rational Thinking Promotes Suspect-friendly Legal Decision Making», in Applied Cognitive Psychology 30, 2016.

RIBEIRO DE FARIA, Jorge, Direito das Obrigações, Volume I, Almedina, 2003.

RODRIGUES, Benjamin Silva, Da Prova Penal, Tomo II, Bruscamente, A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª Edição, Rei dos Livros, 2010.

SCHWEIGHOFER, Erich et al., GDPR & Privacy – APF 2017, Springer, 2017.

SILVA, Hugo Lança, Monitorização da Internet, onde fica o direito à privacidade, Verbo Jurídico, 2006.

SILVA, Sandra Oliveira, Considerações em torno do princípio «nemo tenetur se ipsum accusare»: o arguido como meio de prova contra si mesmo, Faculdade de Direito da Universidade do Porto, 2016, Tese de Doutoramento.

SILVA RAMALHO, David, Métodos Ocultos de Investigação Criminal em Ambiente Digital, Edições Almedina, 2017.

SOUSA PINHEIRO, Alexandre, Privacy e Proteção de Dados Pessoais: A construção dogmática do Direito à Identidade Informacional, Editora AAFDL, 2015.

SKOUMA, G., LÉONARD, L., «On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection». In Reforming European Data Protection Law. [online] Dordrecht: Springer, 2015, pp.35-60 disponível em: https://link.springer.com/chapter/10.1007%2F978-94-017-9385-8_2.

SLOAN, Robert, WARNER, Richard, Unauthorized Access – The Crisis in Online privacy and Security, CRC Press, 2013.

Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide', National Institute of Standards and Technology (NIST) in the US, 2012, disponível em: https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-61-draft-computer-security-incident-handling-guide-2012.pdf.

SUMAN, Anna, et al., «Challenges for Citizen Science and EU Open Science Agenda», in European Data Protection Law Review, Lexxion, 2018.

TAVARES SILVA, Pedro, et. al., Segurança dos Sistemas de Informação, Edições Centro Atlantico, 2003.

TOCCI, R., «Sistemas digitais. Princípios e aplicações», Prentice Hall, 2003-

VAN DER SLOOT, B., «Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities». In Data Protection on the Move. [online] Dodrecht: Springer, 2016, pp.411-436, disponível em: https://link.springer.com/book/10.1007/978-94-017-7376-8#toc.

VAN WEERT, Tom, K. MUNRO, Robert, Informatics and the Digital Society – Social, Ethical and Cognitive Issues, Springer, 2003.

VARGES GOMES, Mário, Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência, Centroatlantico.pt, 2006.

VENÂNCIO, Pedro Dias, Lei do Cibercrime – Anotada e comentada, Coimbra: Coimbra Editora, 2011.

VITAL MOREIRA e GOMES CANOTILHO, José Joaquim, Constituição da República Portuguesa - Anotada - Volume I - Artigos 1º a 107º, Coimbra Editora, 2014.

YU, W., GRIFFITH, D., GE, L., BHATTARAI, S., GOLMIE, N., An integrated detection system against false data injection attacks in the Smart Grid, Security and Communication Networks, 2015.

Legislação

Constituição da República Portuguesa

Carta dos Direitos Fundamentais da União Europeia

Tratado sobre o Funcionamento da União Europeia

Diretiva n.º 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 – revogada.

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)

Diretiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009 que altera a Diretiva/2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações eletrónicas, a Diretiva 2002/58/CE relativa ao tratamento de dados e à proteção da privacidade no setor das comunicações eletrónicas e o Regulamento (CE) n.º 2006/2004 relativo à cooperação entre autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor

Regulamento (UE) 611/2013 da Comissão, relativo às medidas aplicáveis à notificação da violação de dados pessoais em conformidade com a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho relativa à privacidade e às comunicações eletrónicas

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 (Regulamento Geral sobre a Proteção de Dados – RGPD)

Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados

Orientações do Grupo do Artigo 29 / Comité Europeu para a Proteção de Dados

Opinion 03/2014 on Personal Data Breach notification (adopted on 25 March 2014): http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

EDPB Guidelines on Personal data breach notification under Regulation 2016/679", de 3 de outubro de 2017 e revistas em 6 de fevereiro de 2018: http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

Orientações sobre o encarregado de proteção de dados (EPD) do Grupo de Trabalho do Artigo 29.º, revistas e adotadas em abril de 2017, disponíveis em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

Orientações da ENISA

European Network and Information Security Agency (ENISA), Good Practice Guide for Incident Management, 2010, disponível em: http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management.

Recommendations on technical implementation guidelines of Article 4, ENISA, 2012, disponíveis em: https://www.enisa.europa.eu/publications/art4_tech.

ENISA Recommendations for a methodology of the assessment of severity of personal data breaches (2013), disponíveis em: https://www.enisa.europa.eu/publications/dbn-severity

Normas e outras orientações

International Organization for Standardization (ISO) 31000 ¬ Risk management – Principles and guidelines, first edition 2009-11-15: http://ehss.moe.gov.ir/getattachment/56171e8f-2942-4cc6-8957-359f14963d7b/ISO-31000

International Organization for Standardization (ISO), Information technology – Security techniques – Information security incident management, Part 1: Principles of incident management (ISO/IEC 27035-1:2016)

ISO/IEC 27001:2013 *Information technology -- Security techniques -- Information security management systems – Requirements*

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980

Computer Security Incident Handling Guide do National Institute of Standards and Technology/U.S. Department of Commerce, disponível em: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. Entendemos que todas estas fases são igualmente relevantes para as notificações de violações de dados pessoais.

Anexos

Inquérito 1 | Notificações de violações de dados pessoais

1. Ao detetar um comportamento suspeito como um email de um endereço desconhecido e com um link suspeito devo:
    a. Abrir o email e o link para saber se a informação é relevante.
    b. Abrir o email, mas não abrir o link.
    c. Apagar o email sem o abrir.
    d. Não abrir o email e reencaminhá-lo para o departamento de informática.

2. Quando um amigo me pede informações sobre recrutandos, devo:
    a. Facultar-lhe todos os dados que me pedir. Afinal de contas somos amigos.
    b. Não prestar qualquer informação e relembrar-lhe que me encontro obrigado ao dever de confidencialidade.
    c. Prestar-lhe algumas informações, mas não informações sensíveis.

3. Se receber um potencial recrutando que gostava de saber mais informações sobre casos de sucesso de recrutamento, devo:
    a. Mostrar-lhe informações concretas, com exemplos de CV, informações sobre certificados de registo criminal, etc. de outros candidatos.
    b. Apenas indicar em teoria quais os elementos que deve providenciar.
    c. Falar em casos reais, mas sem indicar elementos que permitam identificar outros candidatos.

4. Se um potencial candidato pretender contactar uma pessoa já recrutada através dos serviços da Vitae Professionals para ouvir «na 1.ª pessoa» a sua experiência, devo:
    a. Imediatamente facultar-lhe os dados de contacto de profissionais recrutados pela Vitae.
    b. Contactar primeiramente antigos recrutados pela Vitae e solicitar-lhes a sua autorização para divulgar o seu contacto ao potencial candidato.
    c. Facultar-lhe o nome e o email de um antigo recrutado, mas não o seu número de telefone, nem a sua morada.

5. O que é um Encarregado de Proteção de Dados:
    a. Um software que rapidamente deteta vírus nos computadores.
    b. Uma pessoa responsável pelos temas relacionados com a proteção de dados pessoais.
    c. Uma pessoa designada pela Comissão Nacional de proteção de dados para gerir todas as bases de dados de uma empresa.

6. A Vitae tem um encarregado de proteção de dados?
    a. Sim.
    b. Não.

7. Se receber um email a indicar que a informação do seu computador foi encriptada e para a obter novamente deve pagar um resgate no valor de 350€, devo:
    a. Pagar o regate e não dizer nada a ninguém.
    b. Imediatamente informar o CEO da Vitae.
    c. Telefonar para a polícia judiciária.
    d. Informar imediatamente o encarregado de proteção de dados da Vitae.

8. Se detetar um incidente de segurança, como alguém não autorizado a mexer num dos computadores da Vitae, devo:
    a. Informar imediatamente o encarregado de proteção de dados da Vitae.

b. Deixar passar alguns dias para ver se houve algum incidente e não preocupar desnecessariamente os colegas.
c. Não fazer nada.

9. Posso consultar a informação guardada no Google drive da Vitae numa rede de wi-fi gratuita num centro comercial?
    a. Sim.
    b. Não.

10. Posso consultar informação de trabalho fora do escritório da Vitae?
    a. Sim, se tomar medidas de segurança para que pessoas não autorizadas não acedam a essa informação.
    b. Sim, sem qualquer problema.
    c. Não. A informação não deve sair do escritório.