DPO mag

EDIÇÃO Nº 8
DEZ / 23

APDPO PORTUGAL

www.dpo-portugal.pt

DPO mag

EDIÇÃO Nº 8
DEZ / 23

APDPO PORTUGAL

www.dpo-portugal.pt

DPO | magazine

FICHA TÉCNICA

NOME
DPO | magazine

PROPRIEDADE
APDPO Portugal – NIF 541502835

DIRETORA
Inês Oliveira

EDITOR
Luís Ferreira Mendes

PERIODICIDADE
Semestral

PREÇO
Gratuito

CONTACTO GERAL
geral@dpo-portugal.pt

UM PROJETO APDPO
ISSN 2184-8211

COPYRIGHT

DPO|magazine: a primeira revista do setor na Europa lançada a 28 de outubro de 2020.

Estatuto Editorial

A DPO|magazine é um projeto de informação internacional que visa preencher espaços vazios e acrescentar valor ao campo da proteção e segurança dos dados e da informação.
A DPO|magazine tem carácter digital, é independente e livre, sem interesses partidários ou económicos, e sem estabelecer hierarquias de funções ou de sectores de atividade, nas suas opções editoriais.
A DPO|magazine pauta-se por padrões de exigência na qualidade da informação e do conhecimento que veicula, primeiro garante da sua credibilidade e afirmação.
A DPO|magazine não fixa fronteiras geográficas, culturais ou temporais, recusando situações de sensacionalismo, exploração ou especulação.
A DPO|magazine fomenta o debate consciente e respeitável das grandes questões que se colocam às sociedades atuais, na perspetiva da melhoria do conhecimento.
A DPO|magazine é responsável apenas perante os seus leitores, numa relação marcada pelo rigor, transparência e disponibilidade quotidianas para o estímulo à reflexão e ao conhecimento.

Conteúdo

O Conteúdo da DPO|magazine estará em permanente adaptação, procurando satisfazer a necessidade de melhor exposição dos temas que elegemos para entregar aos nossos leitores.

Presentemente a revista organiza-se em:

| Artigos
| Conteúdos de parceiros
| Debates
| Entrevistas
| Informações institucionais
| Opiniões
| Publicidade
| Reportagens

A QUEM SE DESTINA?

| Administradores e Gestores de Empresas
| Cargos dirigentes da Administração Pública
| Encarregados de Proteção de Dados
| Técnicos de Proteção de Dados
| Técnicos de Compliance
| Advogados, Solicitadores e Agentes de Execução
| Consultores e Auditores
| Economistas e Contabilistas
| Engenheiros informáticos e de Arquitetura de Sistemas
| Especialistas em Proteção e Segurança de Dados
| Especialistas em Segurança Informática e Cibersegurança
| Especialistas em Sistemas de Informação
| Especialistas em Transformação Digital
| Gestores e Analistas de Dados
| Profissionais BAD, da Informação e do Conhecimento
| Técnicos de Informação e Comunicação
| Técnicos de Recursos Humanos

PUBLICIDADE

Dispomos das seguintes opções para inserção de anúncios: | 2 páginas
| 1 página
| 1/2 página horizontal


PORTUGAL

Mensagem da Diretora

Inês Oliveira

Presidente da Direção da APDPO

Diretora da DPO Magazine

Bem-vindos à DPO Magazine n.º 8!

8 edições de um projeto associativo que a Direção da APDPO se orgulha de dirigir!O caminho até aqui tem sido repleto de desafios e o trabalho e esforço diário de todos e cada um de nós está à vista!

Neste número 8 permitam-me partilhar o desafio, enquanto diretora da DPO Magazine, de avivar Colegas a participar e agregar conteúdos e artigos que enriqueçam.

Pessoalmente, sempre estive convicta de que os projetos associativos, porque somam pessoas, conhecimentos e experiências, enriquecem o Todo e valorizam as Partes. Por isso mesmo, me juntei à APDPO e também por isso estive pronta para servir o propósito associativo quando fui eleita presidente da direção da APDPO.

Por inerência, adotei o projeto da DPO Magazine, na expectativa que fortalecesse de conhecimentos e práticas a massa associativa e permitisse à APDPO, não só, mas sobretudo, a mostra do valor dos seus Associados.

Volvidas 8 edições, é com enorme satisfação que lançamos mais uma edição da nossa revista.

Porque Todos, nas lutas diárias, temos dificuldade em disponibilizar um par de minutos para pensarmos os temas que nos movem.

Porque Todos, no papel de profissionais, não conseguimos despender duas horas para escrevermos um artigo com meia dúzia de páginas.

Porque Todos, no seio familiar, temos afazeres que nos distanciam daquele livro ou do ecrã que nos transporta, através de um link, a um texto a ler.

A APDPO agradece o empenho de Todos aqueles que são os pilares destas 8 edições. E certa da continuidade deste projeto, Todos convoca para as próximas edições.

Desejando boas leituras, vemo-nos na próxima edição!

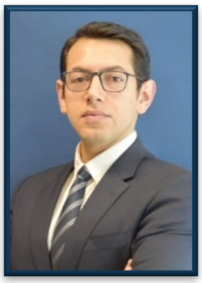
Conteúdo

A articulação entre as competências do Encarregado de Proteção de Dados em entidades públicas e do Responsável pelo Acesso à Informação Administrativa

Augusto Cesar Torbay

Encarregado de Proteção de Dados

Autoridade Nacional de Segurança Rodoviária



Vanda Brites Mendes

Responsável pelo Acesso à Informação Administrativa

Autoridade Nacional de Segurança Rodoviária

A figura do Encarregado de Proteção de Dados (EPD), prevista no art.º 37.º e seguintes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – RGPD), e a do Responsável pelo Acesso à Informação Administrativa (RAI), consagrada no art.º 9.º da Lei n.º 26/2016, de 22 de agosto (Lei de Acesso aos Documentos Administrativos – LADA), embora possuam natureza distinta e não se confundam nas suas atribuições, ambas representam elementos fundamentais na proteção de valores revestidos de dignidade constitucional[1].

Aliás, se tivéssemos de representar graficamente a relação entre as competências do EPD e do RAI, sugeriríamos conceber as respetivas funções como dois círculos parcialmente sobrepostos

[1] Caldeira, M. (2021). Nótula sobre a articulação entre os regimes da LADA e da LPDP. In Freitas, T. & Alves, P. (Org.), *O acesso à informação administrativa* (1.ª ed). Coimbra: Almedina. p. 253.

que, na respetiva área de interseção, possuem em comum a matéria da proteção de dados pessoais. Nesta medida, dedicaremos o presente artigo a refletir sobre essa área de interseção e procuraremos analisar como deve ser realizada a articulação entre as funções do EPD e do RAI.

Como instrumento de promoção da transparência administrativa[2], a LADA vem exigir que a generalidade das entidades que exercem a atividade administrativa pública[3] procedam à designação de um "responsável pelo cumprimento" das respetivas disposições (cfr. art.º 9.º da LADA). Em termos gerais, a este responsável – entenda-se, ao RAI –, compete:

a) A organização e promoção das obrigações de divulgação ativa de informação a que está vinculado o órgão ou a entidade;
b) O acompanhamento da tramitação dos pedidos de acesso e reutilização da informação administrativa; e
c) O estabelecimento da articulação necessária ao exercício das competências da Comissão de Acesso aos Documentos Administrativos (CADA).

Se confrontarmos estas atribuições com as funções que o RGPD – e a Lei n.º 58/2019 de 08 de agosto (Lei da Proteção de Dados Pessoais) – atribuem ao EPD (particularmente no que se refere à relação com os titulares dos dados pessoais), começa a evidenciar-se a existência de um nexo entre os respetivos regimes.

De facto, esta aproximação tem fundamentado o recurso às disposições relativas à posição do EPD para efeitos de integração de lacunas verificadas no regime aplicável ao RAI[4].

Sem prejuízo das questões atinentes ao tratamento de dados pessoais no contexto da divulgação ativa de informação (cfr. art.º 10.º da LADA)[5], é no âmbito das restrições de acesso à informação administrativa com fundamento na proteção de dados pessoais[6] que a tangência entre as competências do RAI e do EPD se torna particularmente evidente.

Manifestando o princípio da administração aberta, o n.º 1 do art.º 5.º da LADA vem estatuir que "*[t]odos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos (…)*"[7]. No entanto, este direito de acesso à informação

[2] Pratas, S. (2020). *A (nova) Lei de Acesso aos Documentos Administrativos* (2.ª ed.). Coimbra: Almedina. p. 120.
[3] Em concreto, as previstas no n.º 1 do art.º 4.º da LADA.
[4] Neste sentido, o Parecer da CADA n.º 65/2020 de 21 de abril.
[5] Veja-se, designadamente, os Pareceres da CADA n.º 368/2022 de 19 de outubro e 336/2022 de 14 de setembro.
[6] Fabião, G. (2021). Restrições de acesso à informação administrativa: dados pessoais. In Freitas, T. & Alves, P. (org), *O acesso à informação administrativa* (1.ª ed). Coimbra: Almedina. p. 209.
[7] Importa notar que a LADA alarga o âmbito constitucionalmente previsto ao acesso à informação administrativa (cfr. art.º 268.º da Constituição da República Portuguesa), não se limitando o respetivo âmbito subjetivo apenas aos "cidadãos" (neste sentido, Pratas, S.

administrativa não é absoluto[8], operando um regime de restrição sempre que se verifique uma das exceções elencadas no art.º 6.º da LADA.

Uma das principais expressões deste regime – e com particular relevância para a presente exposição –, refere-se à restrição do acesso à documentação administrativa que contenha dados pessoais de terceiros (cfr. n.º 5 do art.º 6.º da LADA).

Nos termos da al. b) do n.º 1 do art.º 3.º da LADA, deverá considerar-se como "*nominativo*" o documento administrativo que contenha "*dados pessoais*" (na aceção do ponto 1) do art.º 4.º do RGPD). Como tal, e por via de regra, o acesso a tais documentos deverá encontrar-se reservado apenas aos titulares dos dados pessoais constantes dos mesmos[9].

Contudo, o n.º 5 do art.º 6.º da LADA vem avançar duas exceções à referida restrição de acesso[10].

Por um lado, poderá admitir-se o acesso a documentos nominativos por terceiro caso este se encontre munido de autorização escrita do titular dos dados. Devemos salientar, porém, que a esta autorização deverá ser "(…) *explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que se pretende aceder*" (cfr. al. a) do n.º 5 do art.º 6.º da LADA)[11].

Fora dos casos em que o terceiro possua tal autorização, o acesso poderá ainda ser permitido se o requisitante "(…) *demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação*" (cfr. al. b) do n.º 5 do art.º 6.º da LADA).

Tal como resulta do exposto, a legitimidade do acesso por terceiros a documentos administrativos nominativos deve ser submetida a

(2020). *A (nova) Lei de Acesso aos Documentos Administrativos* (2.ª ed.). Coimbra: Almedina. p. 56).

[8] Com efeito, e tal como referido na doutrina mais autorizada, a própria constituição (cfr. n.º 2 do seu art.º 268.º) procura ressalvar o "*disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal e à intimidade das pessoas*".

[9] De referir, no entanto, é que, nos termos do n.º 8 do art.º 6.º da LADA, os documentos administrativos sujeitos a restrições de acesso com fundamento na proteção de dados podem ser objeto de comunicação parcial sempre que seja possível expurgar os dados pessoais em causa (veja-se, por exemplo, o Parecer da CADA n.º 362/2022 de 19 de outubro).

[10] Devemos realçar, porém, que as exceções a este regime de restrição de acesso não se cingem à LADA. Na mesma ordem se sentido, o Decreto-lei n.º 16/93, de 23 de janeiro (que estabelece o regime da comunicação do geral dos arquivos e do património arquivístico), no respetivo art.º 17.º, vem regular a comunicação do referido acervo de informação quando do mesmo constem dados pessoais.

[11] No caso dos dados de saúde, o n.º 3 do art.º 7.º da LADA vem determinar expressamente que o respetivo acesso por terceiros, mediante consentimento do titular dos dados, deve ser efetuado apenas na medida das informações expressamente abrangidas pelo referido instrumento (sobre esta questão veja-se o Parecer da CADA n.º 38/2023 de 22 de fevereiro).

uma análise cuidadosa de requisitos específicos e pode exigir um sensível juízo de proporcionalidade[12]. Devido às suas atribuições – e principalmente por ser concebido como um elemento facilitador da tramitação dos processos de acesso à informação[13] –, o RAI deve possuir um papel ativo na orientação da organização no exercício destas ponderações[14].

Resulta assim evidente que a atividade do RAI comporta uma especial incidência sobre a matéria da proteção de dados pessoais. Na nossa opinião, atendendo às competências legalmente previstas ao EPD, é nesta sede que se deve estabelecer uma linha de contacto preferencial e corretamente articulada entre ambos os cargos.

Como sabemos, uma das principais funções do EPD é atuar no aconselhamento e informação, não apenas do Responsável pelo Tratamento, mas também dos trabalhadores que atuem no tratamento de dados pessoais (cfr. al. a) do n.º 1 do art.º 39.º do RGPD). Ora, do nosso ponto de vista, a atividade do RAI encontra-se enquadrada no escopo da atuação consultiva do EPD.

Desta forma, e na medida em que o acesso a documentos nominativos deverá ser concebido como uma atividade de tratamento de dados pessoais (na acessão do ponto 2) do art.º 4.º do RGPD) o EPD deverá atuar, em articulação com o RAI, na conformação da mesma com as exigências do RGPD.

Muito embora seja aconselhável que o RAI possua um conhecimento sólido no que se refere à matéria da proteção de dados pessoais, consideramos que os procedimentos das entidades públicas deverão prever mecanismos que possibilitem ao RAI o recurso ao EPD, principalmente no contexto das ponderações mais complexas que eventualmente lhe possam ser exigidas no âmbito da tramitação de pedidos de acesso a documentos nominativos.

Em termos sintéticos, e com fundamento no exposto, podemos afirmar que – embora possuam natureza e propósitos distintos –, as funções do RAI e do EPD não são, em si, antitéticas[15]. Portanto, entendemos que uma correta conjugação de esforços entre estas duas funções importará, sempre, uma clara mais-valia para a tutela dos direitos que servem de substrato às respetivas atribuições.

[12] Como exemplo da complexidade da ponderação exigida na citada norma, veja-se o Parecer da CADA n.º 13/2023 de 18 de janeiro, bem como as respetivas declarações de voto.

[13] Veja-se, designadamente, o Parecer da CADA n.º 49/2022 de 17 de fevereiro.

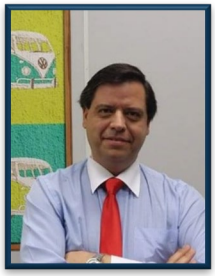
[14] O exposto é particularmente pertinente no contexto do acesso a documentos nominativos que contenham dados pessoais que revelem a origem étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, biométricos ou relativos à saúde, ou dados relativos à intimidade da vida privada, à vida sexual ou à orientação sexual de uma pessoa (cfr. n.º 9 do art.º 6.º da LADA).

[15] Neste sentido, Pinheiro, A. (2015). *Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional*. Lisboa: AAFDL. p 373.

Adequate Technical and Organisational measure

Rui Freitas Serrano

Encarregado de Proteção de Dados



The entire text of the Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation (GDPR) mentions the need for Controllers and Processors to have in place adequate technical and organisational measures to ensure the security and confidentiality of Personal Data under Processing, hence contributing to an operation which complies with the law… and I mean this shows up in the majority of articles and recitals.

WHAT THE LAW READS

What is really meant by suitable, adequate, reasonable and effective measures ?!

The law does, in fact, lay out some reference points and even examples:

- recital 29 - "... pseudonymisation …"

- recital 54 - "... measures so as to protect the rights and freedoms of natural persons …", does not enunciate but it points to very specific nature e.g. mechanism that allows Data Subjects to exercise their rights under the law; measures that prevent the Processing Activities from violating the freedoms of Data Subjects.

- recital 64 - "... verify the identity of a data subject who requests access …", Data Subject identification.

- recital 71 - "... measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised…", data accuracy.

- recital 74 - "... Those measures should take into account the nature, scope, contexto and purposes of the processing and the risk to the rights and freedoms of natural persons …"

- recital 78 - "... implement measures which meet in particular the principles of data protection by design and data protection by default …", be proactive instead of reactive.

- recital 90 - "... a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation …". The notion that the place to start any adequacy process is to perform a Corporate Data Protection Impact Assessment as described under article 35.

- article 6 (2) (b) - "... including measures to ensure lawful and fair processing …"

- article 9 (2) (g) - "... measures to safeguard the fundamental rights and the interests of the data subject …"

- article 24 (2) - "... measures (...) shall include the implementation of appropriate data protection policies …"

- article 25 (1) - "... implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects …"

- article 25 (2) - "... measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons …". As na example, this last ruling leads us to the case of sharing Personal Data on public channels such as Social Media.

- article 34 - this article, although about a circumstance where a severe incident has occurred that affected Personal Data (a Data Breach), has its significant share of mitigation measures both preventive as corrective to ensure that the risk and effective negative impact for Data Subjects is minimised. (3) (a) "... in particular those that render the personal data unintelligible to any person who is not authorised to access it …", which could include pseudonymization, amongst other. (3) (b) "... measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise …"

Let us stop with the examples where we stand.

HOW DID THE MARKET REACT

Acting as part of a team of DPOs which supports corporations in several geographies with their operational compliance towards applicable Personal Data Protection laws (including the GDPR), what we have been experiencing while assessing the compliance of prospective Processors towards our Corporate Clients (acting as the Controller) , regardless of geographic location is a common set of technical and organisational measures.

So, here is what we consistently get back from the assessments towards prospective Processors (meaning what those companies have adopted and implemented on their own):

- RBAC (Role Based Access Control), meaning ensuring that only those users who effectively need access to some specific dataset are granted the credentials that allow such access, and all access credentials are unique and "individual".

- Data Governance as a means to also ensure minimization and adherence to defined retention periods, while documenting applicable Legal Basis and hosting/ sharing destinations.

- Data Localization in the EU has been elected by many which act as Processors to give additional "reassurance" to their Controllers that the Rights and Freedoms of Data Subjects will be observed while Personal Data pertaining to them remains Secure and Confidential.

- Training on Personal Data Protection legislation for all relevant staff (including consultants and, in some cases subprocessors), which inherent degree of acquired knowledge can be proved by a test. "Relevant" meaning those who need to have access to Personal Data.

- Policies and Work Instructions, which allow specific and concrete guidelines so team members can follow operational best practices. Besides a Privacy Policy and respective Privacy Notice on the website, depending on the internal corporate operation it very common to have in place: BYOD (Bring Your Own Device) for those distributed organisations that allows staff to use their own IT assets; Acceptable Use which defines the boundaries for which corporate assets may be used; IT Security to define the basic care to be taken while operating on a "digital" context; other…

- Pseudonymisation is commonly used to segregate direct identifiers (e.g. social security number; email address; phone number; other…) from other data that requires cross-referencing to become Personal Data (e.g. date of birth; preferences on a given subject/ context; annual income; purchase history; other…). It is also commonly used as a means to enable easier "anonymisation".

- Penetration testing shows up consistently in the answers as a "barometer" to assess at regular time intervals the resilience of the Service IT Landscape to potential attacks, as well as to monitor IT Security vulnerabilities.

- Data Segregation by client is a "Privacy by Design" architecture preventive action that is widely adopted by startups to minimise the risk of having Personal Data (as other information) from different clients merging or being accessible due to "bridging".

- Clean Screen enforceability, mainly in those work environments where unauthorised 3rd parties may have access to content displayed on screen.

- Virtual Desktops as secure remote work /access solution that minimises the need to be so demanding regarding local client HW/SW hardening.

These are not "the measures" which need to be in place to ensure an operation which complies with applicable Personal Data Protection legislation, but, they have been "elected" by almost all of the audited prospective Processors (literally over 100 over the last 2 years).

The fact of the matter is that most of these companies are not established in the EU (the prospective Processors, yet many Controllers as well), yet there is a genuine concern and effort to try and adopt the highest standard… I am positive that in many cases this is more "revenue driven" than really a matter of "conscience", because these companies are aware that it is only a matter of time until they may lose a business opportunity because they have not adapted, but still the fact is that many are adopting these common "measures".

WHAT DO OTHER SIMILAR LAWS READ

As we stand, there are many Personal Data Protection laws being effectively enforced around the globe which share similar " Principles " with the GDPR, just to name a few:

- the APPI from Japan

- the PDPB from India - At the very start one may read as one of the aspictures of this law to : "... create a framework for organisational and technical measures in processing of data …"; Chapter VI addresses "accountability measures" article (24) (2) "... review of its security safeguards (...) and take appropriate measures accordingly …"; and still to the point of Data Breaches article 25 (3) "... adopt any urgent measures to remedy the breach or mitigate any immediate harm …"

- the LGPD from Brazil - article 4(IV) (1) "... needs to incorporate necessary and proportional and strictly necessary measures to observe Public Interest …"; article 6 (VII) "... security (...) technical and administrative measures to protect Personal Data from unauthorised access …"; the entirety of article 6 for that matter.

- the LFPD from Mexico - article 19 "... maintain technical, physical and organisational measures that allow protecting personal data from loss, unlawful access, alteration, destruction …"

- the DPA from the Philippines - chapter V Section 20 "... (a) The personal information controller must implement reasonable and

appropriate organisational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing …"; but this law goes further into providing concrete examples:

"...

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorised usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach…"

- the PIPEDA from South Africa - 4.7.3 "... (a) physical measures (...) locked filing cabinets (...) (b) organisational measures (...) security clearances and limiting access on a need-to-know basis …"

Just to provide some examples of "global alignment".

Therefore, as we stand, the market is aligning itself, although not under a "organised endeavour", which accounts for a sintony in the interpretation of the law by teams from across the globe.

Liderlink
Business Solutions

COLOCAMOS A **CIBERSEGURANÇA EM PRIMEIRO PLANO**

Na **LIDERLINK Business Solutions** entendemos a importância de proteger informação e de atender a regulamentações rigorosas de privacidade de dados.

Quem Somos?

Com uma reputação sólida no setor de cibersegurança e um compromisso inabalável com a privacidade de dados, a **LIDERLINK Business Solutions** é a parceira ideal para profissionais que procuram proteger organizações contra ameaças externas.

Como Ajudamos?

Apresentamos sempre uma abordagem personalizada que combinamos com as mais recentes inovações em segurança de dados para garantir uma protecção eficaz dos dados das organizações.

Os Nossos Serviços

Soluções Avançadas

Oferecemos um conjunto completo de soluções de cibersegurança como detecção de ameaças, monitorazação de redes, entre outros.

Segurança Cloud

Mantemos dados seguros na com soluções de segurança personalizadas para ambientes na Cloud.

Recuperação de Dados

Desenvolvemos planos de recuperação personalizados para garantir que as organizações recuperam de eventos inesperados.

FALE CONNOSCO

282 475 763

geral@liderlink.pt
www.liderlink.pt

Quinta do Alto,
Lote 21,
8400-142 Lagoa

O tratamento (i)lícito dos dados pessoais em contexto laboral

Jorge Martinez Batalha

Fundador da Protec Dados
Consultor-Formador
Encarregado da Proteção de Dados (DPO)

Presidente do Conselho Fiscal da APDPO Portugal

https://www.linkedin.com/in/jmbatalhaconsultor/

Como forma de contributo para o reforço da proteção dos dados pessoais dos cidadãos, o presente artigo reflete, em grande medida, a partilha de conhecimento ocorrida no âmbito das «Conversas (In)seguras», em 17 de julho de 2023, data em que se assinalou o 6º aniversário da APDPO, num tema que parece continuar a levantar diversas questões.

Pretende-se, aqui, evidenciar algumas circunstâncias em que, no contexto laboral, o tratamento de dados pessoais pode ser considerado ilícito. Consequentemente, apresentam-se exemplos, sugestões e/ou algumas boas práticas a seguir pelos responsáveis pelo tratamento dos dados.

Apesar do Regulamento Geral sobre a Proteção de Dados (RGPD) ser aplicável desde 25 de maio de 2018, passados cinco anos ainda é notória a diversidade de interpretação do mesmo.

Se olharmos para o artigo 5º do RGPD, a «licitude» corresponde ao primeiro princípio relativo ao tratamento de dados pessoais.

Efetivamente, para que um tratamento de dados pessoais seja lícito tem necessariamente de assentar num dos fundamentos de licitude previstos.

De forma breve, os fundamentos de licitude, previstos no artigo 6º do RGPD, podem ser elencados da seguinte forma:

a) consentimento;
b) contrato ou diligências pré-contratuais;
c) obrigação jurídica;

d) interesses vitais;

e) interesse público ou exercício de autoridade pública;

f) interesses legítimos.

No âmbito dos processos de recrutamento, o recurso ao fundamento de licitude do consentimento dos candidatos continua a ser praticado por várias entidades, públicas e privadas.

Para exemplificar, vejamos os seguintes excertos de documentos incluídos em processos de recrutamento, onde, atualmente, três entidades distintas (optamos por não as identificar) recorrem ao pedido de autorização/consentimento para efeitos de tratamento dos dados dos candidatos:

1. (…) todos os candidatos terão obrigatoriamente que enviar a sua candidatura para o email candidaturasXXXXX@XXXXXXXda.pt, anexando o CV, uma carta de motivação e autorizando (sublinhado nosso) a empresa que conduz o processo de recrutamento (…) a tratar os seus dados ao abrigo do RGPD;
2. (…) informamos que os seus dados serão tratados por XXXXXXXXXX, pessoa coletiva de direito público com o n.º XXX XXX XXX e com sede em XXXXXXXXXXXXXX, XXX-XXX Lisboa, no respeito pelo RGPD, (…) com base no consentimento (sublinhado nosso) e para a seguinte finalidade: Processo de Seleção e Recrutamento;
3. (…) declaro, para os devidos efeitos, que a informação que forneço é correta e verdadeira e dou o meu consentimento (sublinhado nosso) expresso a que a (…) efetue a sua recolha, registo e tratamento, no âmbito do processo de recrutamento suprarreferido.

Olhando para os exemplos anteriores, as seguintes perguntas podem, desde logo, ser colocadas:

1. Atendendo a que os candidatos não poderão abdicar de autorizar/consentir para que o processo de candidatura decorra, estarão os exemplos anteriormente apresentados a incorrer numa atividade de tratamento de dados ilícita?
2. Como poderia um processo de recrutamento decorrer se nenhum candidato desse autorização/consentimento para o tratamento dos dados?

Vamos procurar responder.

Note-se que, nos exemplos anteriores, as expressões «autorização» ou «consentimento» têm, neste contexto, o mesmo significado. A Comissão Nacional de Proteção de Dados (CNPD) refere no seu sítio da internet que "*o consentimento tem de ser inequívoco e corresponder a um ato positivo, explícito, da vontade do titular em autorizar o tratamento de dados*".

Se olharmos para a definição de «Consentimento», constante no artigo 4º, ponto 11), do RGPD, verificamos que corresponde a "*uma manifestação de vontade, livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que*

lhe dizem respeito sejam objeto de tratamento".

O Comité Europeu para a Proteção de Dados (CEPD), nas Diretrizes 05/2020, relativas ao consentimento na aceção do RGPD, afirmava o seguinte:

"*Caso seja obtido em conformidade com o RGPD, o consentimento é um instrumento que permite aos titulares dos dados controlarem se os dados pessoais que lhes dizem respeito vão ou não ser tratados. Caso não o seja, o controlo do titular dos dados torna-se ilusório e o consentimento será um fundamento inválido para o tratamento, tornando essa atividade de tratamento ilícita*" (sublinhado nosso).

A própria Lei 58/2019, no artigo 28º, n.º 3, refere o seguinte:

"*Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais:*

a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou

b) Se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do artigo 6.º do RGPD".

No âmbito das relações laborais, a CNPD também já se pronunciou, de forma genérica e muito simples, sobre o consentimento. Quanto ao contexto laboral, refere no seu sítio da internet o seguinte:

"*no contexto laboral, o consentimento do trabalhador não é um fundamento de legitimidade idóneo. Por um lado, porque devido ao desequilíbrio da relação entre o empregador e o trabalhador, o consentimento não seria efetivamente livre, o que é uma condição essencial para que o consentimento seja considerado válido; por outro lado, porque os tratamentos de dados relativos aos trabalhadores estão na maior parte dos casos previstos e regulados por lei e/ou são necessários para a execução do contrato de trabalho entre o empregador e o trabalhador*".

Ou seja, com o objetivo de contratação do candidato, parece evidente que, para a recolha de dados ser lícita na generalidade dos processos de candidatura, o tratamento de dados pessoais tem por base a necessidade de tomada de diligências pré-contratuais e não o consentimento.

Em suma, o consentimento, em contexto laboral, quando não dado de forma livre, torna essa atividade de tratamento ilícita, tal como vimos referido anteriormente pelo CEPD.

A *Commission Nationale de l'Informatique et des Libertés* (CNIL), autoridade de controlo em França (tal como a CNPD em Portugal), elaborou e publicou, já em 2023, um guia de recrutamento com noções básicas de proteção de dados. Um dos aspetos que o documento procura dar resposta é o seguinte:

Que fundamento jurídico pode ser invocado para realizar um tratamento de dados com a finalidade de recrutamento?

A dada altura, a CNIL refere que, numa determinada entidade, o tratamento efetuado no quadro das próprias operações de recrutamento não pode basear-se no consentimento dos candidatos, uma vez que a recusa da sua parte pode afetar as suas hipóteses de

obtenção de um emprego (ou de determinados tipos de empregos).

Assim, para a generalidade das finalidades, as bases de licitude podem ser as seguintes:

- **Execução do contrato** (medidas pré-contratuais)
- **Interesse legítimo**
- **Interesse público** (para organizações que implementam missões de serviço público destinadas a apoiar as pessoas no regresso ao trabalho e a orientar as empresas no recrutamento, como a APEC e a *Pôle emploi*).

No entanto, quanto à possibilidade do recurso ao «consentimento» nos processos de recrutamento, a CNIL identifica, atualmente, uma exceção. Efetivamente, a escolha da base jurídica do «consentimento» para o tratamento destinado à constituição de uma «biblioteca de currículos» constitui uma evolução das recomendações da CNIL, propostas no sistema de referência relativo à gestão de recursos humanos, que visa uma maior proteção dos dados dos candidatos. Anteriormente, a CNIL recomendava o recurso ao fundamento de «interesse legítimo».

Ainda antes da CNIL ter publicado o referido guia de recrutamento, a *Agencia Española de Protección de Datos* (AEPD), sendo a autoridade de controlo de Espanha, publicou, em 2021, um guia sobre proteção de dados e relações laborais. Neste documento, a questão da desadequação do recurso ao consentimento no âmbito dos processos de recrutamento também é evidente:

"*El tratamiento de datos personales durante el proceso de selección no exige el consentimento de la persona candidata*".

Face ao exposto, recordemos as perguntas a que nos propusemos acima e as respostas que até agora, aqui, evidenciámos:

1. Atendendo a que os candidatos não poderão abdicar de autorizar/consentir para que o processo de candidatura decorra, estarão os exemplos anteriormente apresentados a incorrer numa atividade de tratamento de dados ilícita?

Resposta: Sim, é possível que essas entidades estejam a incorrer numa atividade de tratamento de dados ilícita.

2. Como poderia um processo de recrutamento decorrer se nenhum candidato desse autorização/consentimento para o tratamento dos dados?

Resposta: Seria impraticável proceder a um processo de recrutamento.

Como vimos, para efeitos de conformidade com o RGPD evitando o recurso ao «consentimento», a generalidade dos processos de recrutamento deve seguir boas práticas, entre as quais sugerem-se as seguintes:

1. Informar os candidatos de acordo com o previsto nos artigos 13º (quando os dados pessoais são recolhidos junto do candidato) e 14º (quando os dados não são recolhidos junto do candidato) do RGPD;
2. Identificar apenas uma base de licitude para cada finalidade de tratamento de dados;

3. Recorrer ao pedido de consentimento apenas para os casos em que se pretenda a conservação dos dados para além do processo de candidatura em curso, indicando, claramente, entre outros:
   a) a finalidade (eventual criação de base de dados para futuros processos de recrutamento);
   b) a forma de retirar o consentimento caso assim seja pretendido pelo titular dos dados;
   c) a duração da conservação dos dados;
   d) eventuais partilhas de dados com terceiros;
   e) contactos para exercício de direitos.

Em conclusão, de modo a clarificar a totalidade das melhores práticas a serem seguidas, parece evidente a necessidade de esclarecimento específico por parte da CNPD, em eventual formato de «guia de recrutamento», para que, em matéria de proteção de dados pessoais, o processo de recrutamento se torne claro e inequívoco, tanto para as organizações/empresas como para os cidadãos candidatos a emprego, em contexto nacional.

Terminamos como iniciámos, recordando o primeiro objetivo estratégico indicado no Plano Plurianual de Atividades para o triénio de 2024-2026 aprovado recentemente pela CNPD: é necessário «**contribuir para o reforço da proteção dos dados pessoais dos cidadãos**». Foi o que aqui fizemos

A proteção dos dados pessoais e a segurança da informação

Pedro Santos

CISO/CPO | Presidente Comissão Tecnológica

Município de Portimão | APDPO

1 Introdução e Enquadramento

O artigo 32.º do Regulamento Geral sobre a Proteção de Dados (RGPD), sob a epígrafe "*Segurança do tratamento*" impõe que o(s) Responsável(eis) pelo Tratamento de Dados (RT), levando em conta uma série de parâmetros identificados no n.º 1 do mesmo artigo, devam aplicar as medidas técnicas e organizativas por forma a assegurar um nível de segurança adequado ao risco.

Para as entidades que prestam serviços de telecomunicações eletrónicas acessíveis ao público em redes de comunicações públicas, e no contexto de tratamento de dados pessoais, também já se encontra legislada a adoção de medidas de segurança através do n.º 1 do artigo 3.º da Lei n.º 41/2004, de 18 de agosto que transpõe a Diretiva (UE) 2002/58/CE, de 12 de julho relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas e que decorreria também do artigo 17.º da Diretiva (EU) 95/46/CE, de 24 de outubro, na implementação de medidas técnicas e organizativas na proteção de dados pessoais.

Temos desde 2021 também o Decreto-Lei n.º 65/2021, de 30 de julho que regulamenta o Regime Jurídico da Segurança do Ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de agosto e que transpõe para o regime jurídico nacional a Diretiva (UE) 2016/1148, de 6 de julho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e

da informação em toda a União (Diretiva SRI)[1].

Esta legislação, e em concreto o Decreto-Lei n.º 65/2021, que entrou em vigor no dia 09 de agosto[2], introduz no seu articulado uma série de novas obrigações para um conjunto identificado de entidades, tais como todos os Organismos da Administração Pública (AP), Operadoras de serviços essenciais identificados no Anexo presente na Lei n.º 46/2018, Operadores de infraestruturas críticas e prestadores de serviços digitais. Estas entidades, e entre muitas outras novas obrigações, passaram a ter obrigatoriedades de reporte ao Centro Nacional de Cibersegurança (CNCS), à semelhança do que acontece atualmente com algumas obrigatoriedades de reporte no que à proteção de dados diz respeito, dirigidos à Comissão Nacional de Proteção de Dados (CNPD).

Já no que diz respeito às operadoras de telecomunicações na lei das comunicações eletrónicas no que deriva da Lei n.º 5/2004, de 10 de fevereiro na sua versão atual, e que transpõe para a ordem jurídica nacional a Diretiva (UE) n.º 2002/21/CE, de 7 de março, operacionalizada pelo regulamento da Autoridade Nacional de Comunicações (ANACOM) n.º 303/2019, de 1 de abril, e respeitante à segurança e integridade das redes e serviços de comunicações eletrónicas, é possível encontrar idênticas medidas de implementação e reporte, desta feita para a ANACOM.

Nesta panóplia de legislações, parece ser importante a necessidade de conjugação das responsabilidades e dos deveres nelas previstos com as necessidades e deveres previstos no RGPD[3]. Nesse encalce, será intenção do presente trabalho mostrar algumas especificidades dos regimes aplicáveis, com a importância de analisar possíveis incompatibilidades e conflitos de interesse inerentes ao desempenho da função de responsável de segurança e à de encarregado de proteção de dados, importância das análises de risco nas avaliações de impacto e como um incidente de segurança pode ser uma violação de dados. Esta análise parece ser ainda mais importante, no âmbito em que o cumprimento das obrigações legais respeitantes à segurança da informação e Cibersegurança poderão apoiar e reforçar a conformidade, como por exemplo o estabelecido no n.º 1 e 2 do artigo 32.º do RGPD.

[1] Revogada com efeitos a partir de 18 de outubro de 2024, pela Diretiva (NIS 2) Diretiva (EU) 2022/2555, aguardando-se também por isso alterações na legislação nacional que transpõe a SRI

[22] Os artigos 4.º, 5.º, 7.º e 11.º a 17.º com efeitos só 90 dias após a entrada em vigor, assim como o 9. e 10.º a produzirem efeitos um ano após a entrada em vigor

[3] Diretiva (UE) 2016/1148, considerando 72 "*A partilha de informações sobre os riscos e incidentes a nível do grupo de cooperação e da rede de CSIRT e o cumprimento dos requisitos de notificação de incidentes às autoridades nacionais competentes ou às CSIRT poderão requerer o tratamento de dados pessoais. Esse tratamento deverá cumprir o disposto na Diretiva 95/46/CE do Parlamento Europeu e do Conselho e no Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho. Na aplicação da presente diretiva deverá respeitar-se, consoante adequado, o Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho*"

Sendo esta legislação relativamente recente, para se proceder a um trabalho de investigação neste âmbito que consiga ajudar a dar as respostas pretendidas, os conceitos serão avaliados com recurso à doutrina existente no âmbito de segurança da informação e proteção de dados. Esta será analisada em confronto com o Direito primário identificado e sempre que possível socorrido de Direito secundário que o apoie.

Na leitura da obrigação dos RT de aplicar "*medidas técnicas e organizativas adequadas*" ao nível de segurança e que aparece no n.º 1 do artigo 32.º do RGPD assim como nos artigos 24.º e 25.º do mesmo diploma, ficam algumas questões como *(i) o que se entende por medidas técnicas e organizativas; e (ii) como preencher a locução adequadas?*[4]. Para estas questões e no que concerne às medidas a adotar nas entidades abrangidas pela legislação do Regime Jurídico do Ciberespaço, artigo 14.º, 16.º e 18.º da Lei n.º 46/2018 e pela Lei das Comunicações Eletrónicas, artigo 54.º-A da Lei n.º 5/2004, conseguem-se algumas respostas tais como a necessidade de desenvolver planos de segurança, artigo 7.º do Decreto-Lei n.º 65/2021 e artigo 17.º do Regulamento n.º 303/2019 assim como a efetivação de análises de risco e implementação dos requisitos de segurança, artigo 10.º do Decreto-Lei n.º 65/2021 e artigo 10.º do Regulamento n.º 303/2019. Importa também refletir sobre a diretriz da CNPD 2023/1[5] que identifica claramente, mas não de forma exaustiva, algumas medidas técnicas e organizativas adequadas à segurança dos dados.

É feita uma chamada de atenção à iniciativa que o legislador teve, ao incluir como possivelmente necessário a utilização de medidas mais específicas para cumprimento dos requisitos de segurança, tal como o uso de normas [6] internacionalmente aceites, como por exemplo o poderão ser as da *ISO/IEC International Standard Organization*, como referido no artigo 9.º do Decreto-Lei n.º 65/2021 *"…através da utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia."* [7] ou o n.º 2 alínea b) do artigo 6.º do Regulamento n.º 303/2019 "*Ser baseadas, na ausência das decisões previstas na alínea anterior, nas normas, especificações e recomendações nacionais, europeias e internacionais existentes sobre a matéria…* ", onde depois na sua implementação é devido aplicar o princípio da proporcionalidade

[4] (Cordeiro, Direito da Proteção de Dados, 2020, p. 321)

[5] Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122048

[6] Categorização como *Soft-Law* na combinação da Lei formal com normas técnicas (Freitas, 2021)

[7] Diretiva (UE) 2016/1148, artigo 19.º "*…os Estados-Membros incentivam, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, a utilização de normas e especificações europeias ou internacionalmente aceites plicáveis à segurança das redes e dos sistemas de informação.*"

como um limite ao que o sistema pode exigir do RT[8].

No final, importa realçar o artigo 3.º do Decreto-Lei n.º 65/2021 "*O cumprimento dos requisitos de segurança e das obrigações de notificação de incidentes previstos no Regime Jurídico da Segurança do Ciberespaço e no presente decreto-lei não prejudica:*" e o estipulado na sua alínea a)[9], assim como no n.º 2 do artigo 20.º do Regulamento n.º 303/2019 "*O cumprimento das obrigações de notificação previstas no presente Capítulo I não prejudica, nem substitui, nomeadamente:*" o estipulado na sua alínea a)[10], e que é claramente indicativo que deverá haver uma simbiose das legislações por forma a que não haja comprometimento de uma obrigação em relação a outra[11].

2 Notificações de Violação de Dados e de Incidentes

2.1 Notificação de Violação de Dados

No artigo 33.º do RGPD, epigrafado de "*Notificação de uma violação de dados pessoais à autoridade de controlo*", é estabelecido o dever de notificar a Autoridade de Controlo competente sempre que haja a ocorrência de violação de dados pessoais com risco para os direitos e liberdades das pessoas singulares. No n.º 2 do mesmo artigo, está previsto, por sua vez, a obrigatoriedade do subcontratante notificar o RT, algo que deve ficar plasmado no anexo ou adenda ao contrato de prestação de serviços como imposto pelo n.º 3 alínea f) do artigo 28.º do RGPD. Importante salientar que o RT está isento de efetuar esta notificação *se ela não constituir um "risco para os direitos e liberdades das pessoas singulares". Ele deve, por conseguinte, proceder caso a caso à análise dos riscos envolvidos, antes de proceder à notificação*[12].

No que respeita à adenda ao contrato, será importante seguir as clausulas contratuais standard[13], por Decisão de Execução (UE) 2021/914 da Comissão, de 4 de junho de 2021[14].

No n.º 3 do artigo 33.º do RGPD é indicado o conteúdo mínimo a constar da comunicação, e que deve incluir a descrição da natureza da violação, número de titulares afetados, categoria de registos de

[8] (Cordeiro, Direito da Proteção de Dados, 2020, p. 322)

[9] "*O cumprimento dos requisitos específicos de segurança e das obrigações específicas de notificação de incidentes nos termos definidos pelas autoridades competentes, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC), pela Autoridade Nacional de Comunicações (ANACOM), pela Comissão Nacional de Proteção de Dados (CNPD) e por outras autoridades setoriais, nos termos das disposições legais e regulamentares aplicáveis;*"

[10] "*O cumprimento, por parte das empresas, das suas obrigações de notificação dos incidentes de segurança em causa às autoridades competentes, nomeadamente a ANPC, o Ministério Público, o CNCS, a CNPD…*"

[11] Diretiva (UE) 2016/1148, n.º 1 artigo 2.º "*O tratamento de dados pessoais ao abrigo da presente diretiva é efetuado nos termos da Diretiva 95/46/CE.*"

[12] (Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, 2021, p. 272)

[13] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[14] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

dados pessoais em causa assim como as categorias de titulares.

Na notificação e existindo EPD nomeado, deverão ser comunicados os contatos do mesmo, ou não existindo EPD, deverá ser indicado um outro ponto de contato através do qual possam ser obtidas mais informações por parte da autoridade de controlo. Deverá ser ainda elaborada uma descrição das prováveis consequências da violação de dados, assim como quais as medidas adotadas ou propostas adotar para reparar a violação, e se caso disso, medidas já implementadas ou necessárias implementar para atenuar eventuais efeitos negativos decorrentes da violação.

Importante referir que na necessidade de notificação, existe um prazo de 72 horas após o RT ter tido conhecimento da violação de dados pessoais para notificar a autoridade de controlo. Caso esta notificação não seja efetuada dentro do prazo de 72 horas, assim que o seja e no mais breve curto espaço de tempo, deverá ser acompanhada dos motivos que deram origem ao atraso. Existe ainda a prerrogativa no n.º 4 do artigo 33.º de que caso não seja possível a transmissão de toda a informação exigível na notificação, dentro do prazo estabelecido na norma, o RT possa fasear a sua comunicação, desde que sem demora injustificada.

O Grupo de Trabalho do Artigo 29[15] (GT Art. 29.º), explica que as violações de dados podem ser categorizadas de acordo com três princípios bem conhecidos da segurança da informação[16]:

- «Violação da Confidencialidade» - quando existe uma divulgação ou acesso acidental ou não autorizado a dados pessoais.
- «Violação da Integridade» - quando existe uma alteração acidental ou não autorizada dos dados pessoais.
- «Violação da Disponibilidade» - quando existe uma perda de acesso ou a destruição acidental ou não autorizada de dados pessoais.

Importante notar que apesar desta divisão em três princípios por parte do GT Art. 29.º, uma violação de dados poder-se-á reportar à violação cumulativa de mais do que um destes princípios.

Em relação à violação da disponibilidade, importa esclarecer que poderá existir indisponibilidade no acesso aos dados fora de uma violação, nem sempre a indisponibilidade corresponde a uma violação. Exemplo disso é o que decorre de uma manutenção de sistemas com suspensão de acessos à informação, a não disponibilidade não resulta de um incidente, mas sim de um evento conhecido e programado.

Importa também referir que estas notificações à CNPD de violação de dados, antecedendo o imposto agora no RGPD, já eram obrigatórias pelo artigo 3.º-A da Lei n.º 41/2004 no âmbito das empresas que oferecem serviços de

[15] Aprovadas pelo Comité Europeu para a proteção de dados no *Endorsement* 1/2018 - https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf

[16] (Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, 2018, p. 8)

comunicações eletrónicas ao público, como também já decorreria do artigo 18.º da Diretiva (UE) 95/46/CE.

2.2 Notificação de Incidentes

Na Lei n.º 46/2018, os artigos 15.º, 17.º e 19.º estabelecem a obrigatoriedade de notificação de incidentes com um impacto relevante na segurança das redes e dos sistemas de informação, estando no n.º 4 dos citados artigos fixados os parâmetros da comunicação, cujos requisitos e necessidades são melhor definidos no Decreto-Lei n.º 65/2021 melhor definidos os requisitos e necessidades destas notificações.

No que diz respeito ao Decreto-Lei n.º 65/2021, é no Capítulo IV, artigo 11.º e seguintes que estatui a obrigação de notificação de incidentes, onde se pode ler no n.º 1 do artigo 11.º "*A Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais notificam o CNCS da ocorrência de incidentes com impacto relevante ou substancial nos termos, respetivamente, dos artigos 15.º, 17.º e 19.º do Regime Jurídico da Segurança do Ciberespaço.*". Ao invés do que acontece com a legislação referente à proteção dos dados pessoais, o Decreto-Lei n.º 65/2021 cria no artigo 16.º uma taxonomia de incidentes e de efeitos onde é dada importância à causa e efeito do incidente, e onde apesar de não vir listado no n.º 2 do referido artigo, um dos efeitos poderá ser exatamente o comprometimento de dados pessoais cujo RT seja a entidade onde ocorra o incidente.

O artigo 12.º do Decreto-Lei n.º 65/2021, e relativo às notificações de incidentes de segurança, impõe três fases com notificações diferentes por incidente. Assim temos no artigo 13.º "*Notificação Inicial*" logo que haja conclusão sobre a existência ou que possa vir a existir um impacto relevante ou substancial[17] e até duas horas após essa verificação, sendo o conteúdo a incluir estipulado no n.º 2 do mesmo artigo, e contempla como informação: (i) contatos do representante da entidade, (ii) data do início ou deteção do incidente, (iii) descrição do mesmo, (iv) estimativa de impacto, (v) número de utilizadores afetados e (vi) zona geográfica afetada. Depois no prazo máximo de duas horas logo que deixe de existir impacto relevante ou substancial, artigo 14.º "*Notificação de fim de impacto relevante ou substancial*", com a atualização da informação transmitida como: (i) duração do incidente, que (ii) medidas foram adotadas para a resolução do incidente e (iii) prazo estimado para a recuperação total dos serviços. Por fim e no artigo 15.º estabelece-se a obrigação de se proceder a uma "*Notificação Final*" a ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar, o n.º 2 identifica a informação que deve ser incluída,

[17] No que se refere à segurança das redes e dos sistemas de informação, artigo 15.º, continuidade dos serviços essenciais prestados, artigo 17.º e na prestação de serviços digitais, artigo 19.º da Lei n.º 46/2018

com destaque para a alínea f)[18] e que pressupõe logo à partida que um incidente de segurança notificado ao CNCS, possa ou deva ser notificado também nos devidos termos à CNPD. Ressalvar também que caso o incidente seja resolvido dentro das primeiras duas horas após a deteção, poderão as entidades enviar unicamente a notificação final, n.º 2 artigo 13.º do diploma em referência.

Para finalizar, recordar que esta obrigação decorre da Diretiva SRI, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Esta visa assegurar que os operadores de serviços essenciais e os prestadores de serviços digitais tomam as medidas técnicas e organizativas adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e que notificam as autoridades competentes[19].

De idêntica forma ao estabelecido no Decreto-Lei n.º 65/2021, também o Regulamento n.º 303/2019 no capítulo I artigo 20.º e seguintes, impõe o dever de notificação à ANACOM de violações de segurança ou perdas de integridade com impacto significativo no funcionamento das redes e serviços.

2.3 Observações

Importa perceber aqui o que refere a alínea 12 do artigo 4º do RGPD quando se reporta a uma "*«Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;*" [sublinhado nosso]. Definição esta que que nos leva à alínea c) do artigo 3.º da Lei n.º 46/2018 "*«Incidente», um evento com um efeito adverso real na segurança das redes e dos sistemas de informação;*" [sublinhado nosso]. No mesmo âmbito, na alínea i) do n.º 1 do artigo 2.º do Regulamento n.º 303/2019 encontramos "*«Incidente de segurança», o evento com um efeito adverso real na segurança das redes e serviços, incluindo uma violação de segurança ou perda de integridade;*" [sublinhado nosso]. Podemos em certo sentido concluir que uma violação de dados pessoais é um incidente real que de alguma forma provocou um tratamento acidental ou ilícito de dados pessoais com possível impacto negativo no que respeita aos direitos e liberdades dos seus titulares[20].

"*O que deve ficar claro é que uma violação é um tipo de incidente de segurança. No entanto, como indicado pelo artigo 4.º, alínea 12, o*

[18] "*Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público, à ANEPC, à ANACOM, à CNPD…*"

[19] (Quadro Nacional de Referência para a CiberSegurança, 2019, p. 12)

[20] O EDPS na segunda opinião à Diretiva (UE) 2002/58/EC diz no seu ponto 18 "*The EDPS is pleased to see that the three legislative proposals contain the same definition of security breach notification, which is described as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data, transmitted, stored or otherwise processed…*" (The European Data Protection Supervisor, 6.6.2009, p. 30)

RGPD só é aplicável quando existe uma violação de dados pessoais. A consequência de tal violação é que o responsável pelo tratamento não poderá assegurar o cumprimento dos princípios relativos ao tratamento de dados pessoais, conforme definido no artigo 5.º do RGPD. Isto realça a diferença entre um incidente de segurança e uma violação de dados pessoais – em essência, enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais." [21]

Nem todos os incidentes a notificar ao CNCS ou à ANACOM terão um cariz de risco para os dados pessoais ou mesmo pessoas singulares, sendo que esta avaliação deverá ser sempre efetuada por forma a aferir se, no decorrer de uma violação ou incidente de segurança, não estarão em causa tratamentos ilícitos de dados pessoais com obrigação de ser também notificada à CNPD. Esta notificação à CNPD, a ser feita, será em termos distintos conforme legislação já apresentada, não esquecendo que neste caso, esta notificação à CNPD deverá ser referenciada na notificação final ao CNCS, alínea f) n.º 2 artigo 15.º do Decreto-Lei n.º 65/2021.

Em relação à divulgação de dados pessoais de forma acidental, desconhecimento, inexistência de procedimento/mecanismo estabelecido para todos e cada tratamento de dados independentemente de haver licitude no seu tratamento, que violem os princípios da segurança e os princípios da proteção de dados, poderá ser considerado um incidente de segurança, uma vez que tal consubstancia materialmente uma violação de confidencialidade. No entanto se este tipo de incidente não colocar em causa a segurança das redes e dos sistemas de informação, não haverá necessidade de notificação ao CNCS, podendo, no entanto, ser obrigatória a sua notificação à CNPD se em causa estiverem riscos associados a pessoas singulares.

O prazo de duas horas para a notificação inicial ao CNCS respeitante a um incidente de segurança, permitirá uma janela de 70 horas de avaliação no que corresponde a uma possível violação de dados pessoais com riscos para as pessoas e necessária comunicação à CNPD, com o pendor do cumprimento destes prazos não prejudicarem a mitigação e a resolução do incidente, ao qual se deverá dar prioridade, podendo ser também neste sentido um dos motivos possíveis de apresentar à CNPD de acordo com o n.º 1 do artigo 33.º do RGPD *"…Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso."*.

Em relação ainda às notificações, importa também referir o artigo 34.º do RGPD, que obriga a que no caso da violação de dados pessoais for suscetível de implicar elevado risco para os direitos e liberdades das pessoas singulares, o RT comunica a violação de dados pessoais ao titular sem demora justificada. Esta notificação no entanto e em determinadas situações, pode ser através de uma comunicação

[21] (Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, 2018, p. 7)

pública, alínea c) n.º 3 do artigo 34.º. Já a Lei n.º 41/2004 no artigo 3.º-A no seu n.º 2 indicavam obrigação idêntica "*Quando a violação de dados pessoais (…) devem ainda, sem demora injustificada, notificar a violação ao assinante ou ao utilizador, para que estes possam tomar as precauções necessárias.*"

A conjugação das obrigações de notificação em ambos os regimes em análise, Proteção de Dados e Cibersegurança, poderia levar à comunicação ou exposição pública de incidentes de segurança, que ao invés de a ajudar a resolver podem agravar a situação e dificultar a celeridade da sua resolução. Neste aspeto, e por necessidade de mitigar esse risco, a obrigatoriedade de notificação ao CNCS em conjugação com o disposto no n.º 8 do artigo 2º da Lei n.º 46/2018 "*A presente lei não prejudica as medidas destinadas a salvaguardar as funções essenciais do Estado, incluindo medidas de proteção da informação cuja divulgação seja contrária aos interesses de segurança nacional, à manutenção de ordem pública ou a permitir a investigação, a deteção e a repressão de infrações penais*", na avaliação do cumprimento imediato e sem demora do estipulado no artigo 34.º do RGPD, entende-se que possa ser uma justificação de não cumprimento deste.

Para terminar a observação fica a citação de Diogo Lopes Alves[22] "*A própria definição de violação de dados pessoais no RGPD refere que se trata de uma violação da segurança, donde se infere que a Cibersegurança é um imperativo normativo que demonstra a proximidade entre a proteção de dados pessoais e a segurança, realçando a importância de uma abordagem coordenada entre as duas para identificar e gerir os riscos, consequentemente, aumentando a eficácia e reduzindo os esforços*".

3 Avaliações de Impacto e Análises de Risco

3.1 Avaliação de Impacto sobre a Proteção de Dados

As Avaliações de Impacto são instrumentos de responsabilização e demonstração de conformidade, sendo obrigatórios nos termos do artigo 35.º do RGPD, desde logo e sempre que o tratamento de dados seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas baseado no novo paradigma assente na análise de risco. Além deste resultado de análise de risco previsto no n.º 1 do artigo 35.º do RGPD e das orientações do GT Art. 29.º[23], a CNPD elaborou o Regulamento n.º 1/2018[24] relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que elenca a sua obrigatoriedade em nove situações distintas.

A AIPD deve incluir toda a informação relevante sobre o

[22] (O papel fundamental da Cibersegurança na Proteção de Dados Pessoais, 2021, p. 126)

[23] (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, 2017, pp. 10-11)

[24] Consultado a 20 de outubro de 2021 em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818

tratamento, e pelo menos as determinadas no n.º 7 do artigo 35.º do RGPD, que, nas suas alíneas c) e d) preveem: "*Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.º 1;*" e na alínea d) "*As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa*." [sublinhados nossos].

Quando se fala em AIPD, e decorrente da própria leitura do n.º 1 do artigo 35º, que refere, "*…for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares…*", é colocado o foco em todas as pessoas singulares, não só nos titulares dos dados que possam ser alvo de operações de tratamento. Importa perceber por exemplo que o tratamento de dados pessoais de uma pessoa singular no âmbito de atribuição de apoio social, pode impactar com os direitos e liberdades das pessoas singulares que com este coabitem, mas cujos dados não são "diretamente" tratados. Assim, é importante na elaboração da AIPD, a análise do risco respeitante a possíveis ameaças ou repercussões em pessoas singulares e não só aos titulares cujos dados serão alvo de tratamento.

Quando se fala em riscos e repercussões relativas aos direitos e liberdades das pessoas singulares, devemos dar especial atenção ao considerando 75 do RGPD, o qual se reporta, em especial, a "*…operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social….*", e é com base em todos estes riscos e na medida dos mesmos que o RT na elaboração do AIPD deverá determinar os cuidados a ter.

"*Uma AIPD é um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para fazer face a esses riscos*"[25]

No que respeita aos elementos a avaliar na AIPD, o considerando 90 do RGPD refere que "*…a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.*"

[25] (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, 2017, p. 4)

[sublinhado nosso], não sendo, no entanto, imposta forma ou estrutura.

A norma ISO/IEC 27701:2019[26] no ponto 7.2.5 *Privacy impact assessment*, na aplicação da norma por remissão ao n.º 2 do artigo 9.º do decreto-Lei n.º 65/2021, diz que a organização deve efetuar as avaliações de impacto de privacidade quer em novos processamentos de PII (*Personal Identifiable Information*)[27] quer na necessidade ou planeamento de alterar processamentos já existentes de PII. Na norma, a necessidade de ser efetuada a Avaliação de Impacto da Privacidade, decorre da necessidade de avaliar os riscos que o processamento de PII traz às pessoas singulares cujos dados serão envolvidos no processamento, fazendo remissão para as diversas legislações que podem inclusive definir os casos em que isso acontece, alinhando-se assim com o RGPD.

3.2 Análise de Risco

Na Lei n.º 46/2018, nos artigos 14.º, 16º e 18.º é determinado o dever de implementar as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e sistemas de informação. Estas medidas devem garantir que na ocorrência de incidentes o seu impacto seja reduzido ao mínimo.

No Decreto-Lei n.º 65/2021, Capítulo III, temos a iniciar no artigo 9.º, a indicação das medidas para cumprimento dos requisitos de segurança, e depois no n.º 1 do artigo 10.º a consagração do dever de elaborar análises de risco relativas aos ativos que garantam a continuidade. Estas análises deverão ser efetuadas anualmente, após notificação de um risco por parte do CNCS ou sempre que haja alterações ou ocorrências nos sistemas que possam inserir novos riscos ou alterar os riscos associados.

Já na Lei n.º 5/2004, no artigo 54.º-A também é indicado o dever de adotar as medidas técnicas e organizacionais adequadas à prevenção, gestão e redução dos riscos para a segurança das redes e serviços, indo ao encontro do que será o propósito de uma gestão de risco.

Mais uma vez, e também no Regulamento n.º 303/2019, alínea a) do n.º 1 do artigo 6.º, é previsto a necessidade de adotar medidas técnicas e organizativas resultantes do processo de gestão e redução dos riscos para a segurança das redes e serviços. No entanto e além do foco na entidade no que se refere a incidentes de segurança, e como é referido "*…impacto dos incidentes de segurança nas redes interligadas, a nível nacional e internacional, e nos utilizadores…*" [sublinhado nosso] o impacto nos utilizadores que poderão ser pessoas singulares, também deverá ser apurado e impedido ou minimizado.

Gestão do Risco, na leitura de José Carlos Lourenço Martins[28] no âmbito da segurança da informação e Cibersegurança, *consiste no conjunto de atividades que de forma*

[26] (ISO/IEC 27701:2019, 2019, p. 31)

[27] ISO/IEC 29100:2011 "*any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal*"

[28] (Gestão de Segurança e Cibersegurança nas Organizações, 2021, p. 216)

integrada e coordenadas procuram identificar, analisar, avaliar e tratar os riscos de uma Organização, onde o risco é o efeito da incerteza na consecução dos objetivos e consiste na probabilidade/possibilidade de uma ameaça ocorrer, através da exploração de uma ou mais vulnerabilidades em um ou mais ativos de uma Organização e o impacto que possa causar.

A gestão do risco de Segurança da informação e Cibersegurança é todo ele por si um complexo sistema que merece uma abordagem independente. Segundo a ISO/IEC 27005:2018[29], ponto 5 *Background*, por forma a identificar os requisitos necessários ao garante da segurança da informação e criação de um sistema efetivo de gestão da segurança da informação, é necessária uma abordagem sistémica na gestão do risco por forma a identificar as necessidades organizacionais. Nesta abordagem, o foco é a organização e a segurança dos seus ativos, o esforço nas medidas de segurança deve estar alinhado na gestão do risco de forma eficaz, oportuna e onde elas forem necessárias. Ainda na mesma norma internacional pode-se perceber que a gestão de risco deve analisar o que pode acontecer e quais as possíveis consequências de tais acontecimentos, isto antes de haver decisão sobre o que deve ser feito por forma a reduzir o risco a um nível aceitável.

A gestão de risco parte desde logo da identificação dos ativos, que possam ser essenciais na prestação dos serviços, n.º 1 do artigo 10.º do Decreto-Lei n.º 65/2021 "*… devem realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação…*" e desde logo do inventário obrigatório pelo artigo 6.º do mesmo Decreto-Lei, assim como dos artigos 8.º e 9.º do Regulamento n.º 303/2019.

3.3 Observações

De notar que as análises de risco diferem das AIPD no que se refere ao alvo ou foco em análise, sendo que numa análise de risco o foco é a entidade e o valor dos seus ativos relativamente às ameaças e vulnerabilidades identificadas, numa AIPD o foco são as pessoas singulares no que se refere às suas liberdades e garantias, "*… a AIPD ao abrigo do RGPD é um instrumento que visa gerir os riscos para os direitos dos titulares dos dados e, como tal, avalia-os na perspetiva destes últimos, como acontece em determinados domínios (p. ex. segurança societal). Em contrapartida, a gestão dos riscos noutros domínios (p. ex. segurança da informação) centra-se na organização.*"[30]

Importa, no entanto, ressalvar, que não é possível efetuar uma AIPD sem conhecer os riscos associados aos ativos utilizados no tratamento dos dados pessoais, sendo que a gestão de risco inerente a estes, já seria necessária por questões de segurança na legislação de proteção de dados, até porque não é possível identificar as

[29] (ISO/IEC 27005:2018, 2018, p. 2)

[30] (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, 2017, p. 20)

consequências para os direitos, liberdades e garantias das pessoas singulares se não se garantir a segurança dos ativos que processam os dados pessoais.

O GT Art.29.º, dá uma definição de risco para enquadrar a importância deste nas AIPD, "*Um «risco» é um cenário que descreve um acontecimento e as respetivas consequências, estimado em termos de gravidade e probabilidade. Por outro lado, a «gestão do risco» pode ser definida como as atividades coordenadas que visam direcionar e controlar uma organização no que toca ao risco.*"[31]

"*Cabe ao RT proceder a uma análise objetiva que atente a todos os elementos relevantes, com destaque para a natureza e a origem dos dados, para o âmbito e o contexto em que o tratamento é realizado e para as finalidades prosseguidas ou para o possível impacto de um determinado ato na esfera jurídica dos titulares de dados afetados. Quanto maiores os riscos envolvidos, maiores serão, naturalmente os cuidados a ter.*"[32] Na ponderação destes riscos, se os mesmos forem considerados elevados para os direitos e liberdades de pessoas singulares, o RT deve nos termos dos artigos 35.º e 36º do RGPD, proceder à elaboração de uma AIPD.

Importa também ressalvar que, em relação às análises de risco, está estipulado no n.º 1 do artigo 10.º do Decreto-Lei n.º 65/2021 o momento em que estas devem ser efetuadas. Neste sentido, importa alertar que sempre que uma análise de risco indique alterações relevantes que possam impactuar com uma AIPD já feita, esta deverá ser atualizada em conformidade e no referente a ameaças, valores dos ativos ou novas vulnerabilidades no que respeita às pessoas singulares.

É também interessante. analisar a definição de Avaliação de Impacto de Privacidade oferecida pela ISO/IEC 29134:2017, onde não é feita referência à privacidade para as pessoas singulares, ou mesmo para os titulares de dados, mas só colocada em causa o potencial risco que um sistema que processe PII, pode ter em termos de privacidade.

"*A privacy impact assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, programme, software module, device or other initiative which processes personally identifiable information (PII) and, in consultation with stakeholders, for taking actions as necessary in order to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001. A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and*

[31] (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, 2017, p. 7)

[32] (Cordeiro, Direito da Proteção de Dados, 2020, p. 319)

even after, the project has been deployed."[33]

Assim, interessa reforçar a ideia que a AIPD deve levar em conta não só os riscos para a privacidade, mas também os riscos para pessoas singulares identificáveis, inclusive possíveis riscos para a integridade física decorrentes do tratamento de dados pessoais, que até poderão não ser da pessoa singular titular desses dados. Efetuar uma análise de risco a um ativo, onde a importância com a privacidade tem de ser levada em conta, será só uma das componentes na elaboração da AIPD.

Com respeito ao inventário de ativos, previsto no artigo 6.º do Decreto-Lei n.º 65/2021, e sobre os quais a gestão de risco na avaliação de risco deverá recair, sem esquecer que os próprios recursos humanos e a própria informação e dados tratados poderão ser também estes, ativos críticos da entidade, devendo ser classificados em termos de segurança como tal[34].

Importa no que respeita à elaboração das AIPD, reforçar que esta não será da responsabilidade do EPD, devendo, no entanto, ser-lhe solicitado parecer e orientações sobre as mesmas, artigo 35.º n.º 2 e alínea c) n.º 1 do Artigo 39.º do RGPD. Esta observação torna-se bastante relevante na medida em que poderá resultar num conflito de interesses ou num resultado ambíguo caso seja o EPD a elaborar os AIPD e depois sobre os mesmos ter de emitir parecer e orientações.

Observa-se assim que os regimes de Cibersegurança no que respeita às análises de risco, vêm reforçar e complementar o regime sobre proteção de dados. Aqui importa perceber que as análises de risco focam nos ativos da entidade, e as AIPD por sua vez, focam nas pessoas singulares afetadas por operações de tratamento de dados feitos pela entidade, sejam recursos humanos da própria, clientes, fornecedores ou quaisquer outras. A elaboração de AIPD deve tomar por base as análises de risco, pois são estas que gerem os riscos inerentes aos ativos usados no tratamento dos dados, riscos estes a ser mitigados por forma a reduzir possíveis impactos negativos nos direitos, liberdades e garantias das pessoas singulares.

4 Encarregado de Proteção de Dados e Responsável de Segurança

4.1 Encarregado de Proteção de Dados

Prescreve o artigo 37.º n.º 1 do RGPD que "*O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados…*", sendo a sua obrigatoriedade aplicada a todos os Organismos Públicos e Autoridades, excetuando tribunais no exercício da sua função jurisdicional, (cf. alínea a) do n.º 1 do artigo 37.º do RGPD e artigo 12.º da Lei n.º 58/2019, de 8 de agosto). Nos casos em que o RT não se enquadre no tipo de entidades já mencionadas[35], a nomeação pode ser opcional para os que assim acharem conveniente, ou

[33] (ISO/IEC 29134:2017, 2017, p. IV)
[34] (ISO/IEC 27005:2018, 2018, p. Anexo B)
[35] Organismos Públicos e Autoridades, alínea a) do n.º 1 do artigo 37º do RGPD

obrigatória mediante a análise de alguns requisitos (cf. alínea b) e c) do n.º 1 do artigo 37.º do RGPD e artigo 13.º da Lei n.º 58/2019). Esta designação deve ser comunicada à autoridade de controlo, em Portugal a CNPD, n.º 7 do artigo 37.º do RGPD.

O EPD verifica a conformidade com o RGPD, constituindo uma espécie de "controlo" de primeiro nível, o que apesar de ser exercido com independência, não deixa de ser um controlo interno, porque efetivado ainda dentro das instituições[36]. O EPD servirá, quase como "uma autoridade de autocontrolo"[37] dentro de cada RT ou Subcontratante que esteja obrigado a nomear ou que pretenda nomear um (tendo assim o papel de vigilante que o legislador comunitário quis transmitir para os próprios RT e Subcontratantes)[38].

"*A teleologia subjacente à imposição obrigatória do EPD é a de que em certos casos exista, na organização que procede ao tratamento de dados, uma função especializada no controlo relativamente ao compliance de proteção de dados. Essa função de controlo não dispensa que o cumprimento caiba, em primeira linha, a toda a organização, que deve estar estruturada, desde a conceção e por defeito, para assegurar o cumprimento do Direito de Proteção de Dados. O EPD funciona como uma segunda linha de defesa, que é complementar à atividade de supervisão da autoridade de controlo e, simultaneamente, um provedor dos titulares dos dados (artigo 38.º/4).*"[39]

Em termos hierárquicos[40] e funcionais, o EPD deve ser posicionado por forma a que as suas funções não se confundam com as de RT, e nem destes receba orientações sobre as mesmas, pelo que não lhe é conferida a capacidade de determinar finalidade e meios no tratamento de dados pessoais, nem sequer a possibilidade de o fazer por conta do RT.[41]

Na leitura do n.º 1 do artigo 39º do RGPD, o EPD possui cinco funções principais, sendo elas:

- Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que processem dados, a respeito das suas obrigações nos termos do RGPD e demais legislação aplicável no âmbito da Proteção de Dados;
- Controlar o cumprimento do RGPD, da demais legislação inerente aplicável e das políticas das próprias entidades relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal nas

[36] (O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas, 2020, p. 48)
[37] (CiberLay - As AIPD, o EPD e a Certificação no novo RGPD, 2021, p. 30) "*Este encarregado da proteção de dados surge como uma figura híbrida nesta relação jurídica pois, por um lado, surge no organograma da entidade responsável pelo tratamento e, pelo outro, as suas funções assemelham-se como intermediária e um "agente" da Comissão Nacional de Proteção de Dados* "
[38] (Da responsabilidade do Encarregado de Proteção de Dados, 2020, p. 26)
[39] (Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, 2021, p. 290)
[40] (Onde fica o DPO dentro das Empresas, 2021)
[41] (Direito da Proteção de Dados, 2020, p. 370)

operações de tratamentos de dados, e as auditorias correspondentes;
- Prestar aconselhamento, quando lhe seja solicitado, relativo à AIPD e controlar a sua realização, nos termos do artigo 35.º;
- Cooperar com a autoridade de controlo;
- Atuar como ponto de contacto com a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º; devendo consultar a autoridade de controlo sempre que se justifique.

No âmbito do n.º 4 do artigo 38.º do RGPD também é entendível que fará parte das funções do EPD o relacionamento com os titulares dos dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais, o que é reforçado também na alínea c) do artigo 11.º da Lei n.º 58/2019.

Na Lei n.º 58/2019, ainda no artigo 11.º "*Funções do Encarregado de Proteção de Dados*" na alínea a) é atribuída a função de "*Assegurar a realização de auditorias, quer periódicas, quer não programadas;*", que poderá deixar em aberto a necessidade do EPD efetuar auditorias, o que não é consensual que estas possam ser realizadas pelo EPD. O EPD deverá limitar-se a tudo fazer para que sejam realizadas auditorias, tal como defendido por Diogo Pereira Duarte [42] e por A. Barreto Menezes Cordeiro[43] que nos dizem que ao EPD apenas cabe monitorizar a realização de auditorias, mas já não lhe cabe efetuar a sua realização. A orientação da não realização de auditorias por parte do EPD decorre também do parecer 20/2018 da CNPD[44] onde é dito que "*ao atribuir ao EPD a função de «[a]ssegurar a realização de auditorias, quer periódicas, quer não programadas» parece contradizer o vertido na alínea b) do n.º 1 do artigo 39.º do RGPD, que prevê apenas que o encarregado de proteção de dados controle a conformidade com o presente regulamento (…) e com as políticas do responsável pelo tratamento (….) incluindo (…) as auditorias correspondentes.*", tendo sido solicitado a sua eliminação do texto da proposta, o que não veio a acontecer, ficou a mensagem que o seu conteúdo colide neste aspeto com o plasmado no RGPD.

O GT art. 29.º, dá como exemplo de instrumentos de responsabilização para facilitar a conformidade, a efetuação ou viabilização de auditorias por parte do EPD[45], o que parece ser uma atribuição de competências de auditor ao EPD. No entanto esta posição deve ser lida de uma forma mais restrita em relação à palavra auditoria, numa perspetiva de inspeção, análise e conformidade em colaboração com outras áreas chave dentro da entidade, na gestão do risco dentro de uma segunda linha de defesa, e não na

[42] (Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, 2021, p. 585)
[43] (Direito da Proteção de Dados, 2020, p. 375)
[44] (Parecer à Proposta de Lei n.º 120/XIII/3.ª Gov, 2018, p. 8v)
[45] (Orientações sobre os Encarregados da Proteção de Dados (EPD), 2017, p. 5)

terceira linha[46] como auditor, como também nos parece decorrer das orientações sobre as funções do encarregado de proteção de dados, emanadas da CNIL[47] "*…Esta missão deve assumir a forma de auditorias organizadas pelo EPD (auditoria externa ou interna), ou mediadas pessoalmente pelo EPD, em colaboração…*" [tradução nossa].

4.2 Responsável de Segurança

Cabe no âmbito do Decreto-Lei n.º 65/2021 no artigo 4.º, a indicação de, pelo menos um ponto de contato permanente com o CNCS para a garantia dos fluxos de informação a nível operacional e técnico. No artigo 5.º estabelece-se o dever de designação de um responsável de segurança, com a responsabilidade de gestão das medidas adotadas em matéria de requisitos de segurança. Esta obrigatoriedade engloba toda a AP, operadores de serviços essenciais, infraestruturas críticas e prestadores de serviços digitais (cf. n.º 1 do artigo 2.º da Lei n.º 46/2018 conjugado com o n.º 1 do artigo 2.º do Decreto-Lei n.º 65/2021). Estas designações devem ser comunicadas ao CNCS, n.º 3 do artigo 4.º e n.º 2 do artigo 5.º do Decreto-Lei n.º 65/2021.

Já no Regulamento n.º 303/2019 no artigo 14.º "*Responsável da Segurança*", encontramos novamente o dever de designação para as entidades abrangidas pelo Regulamento (cf. n.º 1 e 2 do artigo 54-A da Lei n.º 5/2004), com a diferença de se poder também designar um adjunto por questões de ausência do responsável da segurança.

Quanto às funções do responsável de segurança, o Decreto-Lei n.º 65/2021 dá algumas indicações das suas funções, iniciando no n.º 1 do artigo 5.º "*As entidades devem designar um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes, nos termos do Regime Jurídico da Segurança do Ciberespaço e do presente decreto-lei.*" [sublinhado nosso], onde se identifica a responsabilidade na gestão das medidas adotadas no garante da segurança da informação e notificação de incidentes. No n.º 1 do artigo 6.º "*As entidades devem elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação dos respetivos serviços, devendo o mesmo ser assinado pelo responsável de segurança.*" [sublinhado nosso], onde se deduz ser do responsável de segurança a responsabilidade de garantir a exatidão do inventário de ativos essenciais na prestação dos serviços de cada entidade. No n.º 1 do artigo 7.º "*As entidades devem elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo responsável de segurança, …*" [sublinhado nosso] o responsável de segurança tem aqui também responsabilidade de validar o plano de segurança desenhado e documentado pela

[46] (Guidance on the 8th EU Company Law Directive - Directive 2006/43/EC – Art. 41-2b, 2010, pp. 9,10)

[47] "*Le DPO est investi d'une mission de contrôle du respect du RGPD. Cette mission doit prendre la forme de vérifications organisées par le DPO (audit externe ou relais interne), ou menées par le DPO personnellement, en collaboration avec les autres fonctions clefs telles que le RSSI (responsable de la sécurité des systèmes d'information)* (Guide Pratique RGPD, Délégués à la protection des données, 2021, p. 6)

entidade, onde deverá constar inclusive a identificação do próprio responsável de segurança, alínea c) do n.º 1. Já no n.º 2 do artigo 8.º "*As entidades devem remeter o relatório anual ao CNCS, devidamente assinado pelo responsável de segurança,* …" [sublinhado nosso], também nos leva a identificar que é da sua responsabilidade garantir que este relatório seja feito e por si validado.

Já quanto à identificação das funções de responsável da segurança no Regulamento n.º 303/2019, decorre diretamente da definição alínea m) do artigo 2.º[48] e das alíneas a) e b) do n.º 1 do seu artigo 14.º[49]. Depois, e à semelhança do que acontece no Decreto-Lei n.º 65/2021, no artigo 9.º do Regulamento n.º 303/2021 o inventário de ativos deve ser assinado pelo responsável da segurança, artigo 17.º o plano de segurança deve ser assinado também pelo responsável da segurança e onde conste a documentação que demonstre o seu mandato, artigo 19.º o relatório anual de segurança também a dever ser assinado pelo responsável da segurança e no n.º 8 do artigo 22.º o dever de assinar a notificação final em caso de incidente.

Importante analisar uma das funções do responsável da segurança no Regulamento n.º 303/2019, e que diz respeito à sua participação no procedimento de auditoria imposto pelo artigo 54.º-F da Lei n.º 5/2004 e artigo 25.º do Regulamento n.º 303/2019. Tais funções estão estipuladas no Regulamento n.º 303/2019, no n.º 2 do artigo 30.º "*As empresas devem apresentar à ANACOM a proposta de auditoria, assinada pelo responsável da segurança:*" [sublinhado nosso], alínea b) do n.º 4 do artigo 32.º "*Enviar à ANACOM cópia do relatório da auditoria, assinado, dele tomando conhecimento, pelo responsável da segurança, …*" [sublinhado nosso] e no n.º 1 do artigo 33.º no que respeita ao plano de correção a ser enviado para a ANACOM devidamente assinado pelo responsável da segurança.

Sobressai assim a qualidade de gestor das medidas em segurança, onde deve garantir a qualidade dos inventários, documentação do plano de segurança, elaboração do relatório anual e responsabilidade no seguimento e validação de auditorias. Será neste ponto importante entender o papel de um "gestor", assim como qual o papel de um *Chief Information Security Officer* (CISO), que parece ser o que pretende ser criado com a designação de um responsável de segurança no âmbito da segurança de redes e sistemas de informação e comunicação.

Segundo José Carlos Lourenço Martins[50] quando se fala em gestão relacionada com a segurança, fala-se em gestão operacional e que são o "Planear, Organizar, Dirigir e Controlar" todas as atividades e esforços no âmbito da Segurança

[48] "*«Responsável da segurança», o colaborador da empresa responsável pela gestão da segurança das redes e serviços e pela sua representação no exercício das funções que lhe são cometidas pelo presente regulamento, nomeadamente nos termos previstos no artigo 14.º;*"

[49] "*… entre os demais deveres previstos no presente regulamento, cabe: a) A gestão da política de segurança; b) A gestão do conjunto das medidas adotadas em matéria de segurança das redes e serviços ao abrigo do disposto na lei e no presente regulamento.*"

[50] (Gestão de Segurança e Cibersegurança nas Organizações, 2021, p. 241)

da Informação a realizar em todas as áreas ou processos em todos os níveis da Organização (estratégico, tático e operacional). Em relação ao responsável de segurança, na mesma obra[51] como CISO, deverá ser visto como um estratega que deve fazer uso da sua criatividade para desenvolver estratégias, definir objetivos a longo prazo, identificar e coordenar as mudanças estratégicas a executar no âmbito da segurança. Conseguir traduzir a visão e a estratégia de alto nível em um plano de ação, conseguindo defender eficazmente a estratégia através da comunicação, colaboração, negociação, motivação e persuasão.

4.3 Observações

A capacitação do responsável de segurança para a gestão a todos os níveis de tudo o que tenha a ver com a segurança das redes, sistemas de informação e comunicação, inclusive com a determinação de planos de correção derivados de auditorias, afasta logo à partida a possibilidade de um EPD nomeado poder executar tais funções. Independentemente das capacidades técnicas e conhecimentos que possa possuir para o exercício das funções, o EPD não poderá, numa primeira leitura, desempenhar as funções de responsável de segurança por conflito de interesses.

O responsável de segurança, como gestor das medidas em matéria de requisitos de segurança, e derivado das funções já indicadas na função de CISO, em que deverá determinar os meios e formas, procedimentos, políticas e controlos aplicados à segurança de redes e sistemas de informação, é algo que o EPD estará impossibilitado de fazer. A efetivação de um sistema de gestão de segurança da informação envolve efetivamente que o responsável de segurança deva determinar finalidades e formas de tratamento de dados pessoais necessários por exemplo aos processos de controlo de acessos, e que teria depois como EPD de avaliar.

Barreto Menezes Cordeiro, ao afirmar que "*No afastamento de situações conflituosas, a autoridade designadora deve considerar as funções já desempenhadas pelo potencial EPD, por exemplo, se é responsável pela segurança informática, pela otimização de procedimento internos relacionados com o tratamento de dados pessoais ou pelo tratamento dos dados pessoais dos trabalhadores. Em todos estes casos parece existir um conflito de interesses.*"[52] [sublinhado nosso], coloca ainda em conflito não a acumulação em si, mas também a hipótese das funções desempenhadas anteriormente pelo EPD poderem ser geradoras de conflito, onde se destaca a de responsável de segurança.

Caberá ao EPD poder avaliar as opções e emitir parecer ou orientações no que à segurança dos dados pessoais, direitos e liberdades das pessoas singulares diz respeito, ajudando assim na melhor definição dos meios a definir pelo responsável de segurança, não devendo por isso o EPD avaliar

[51] (Gestão de Segurança e Cibersegurança nas Organizações, 2021, pp. 248,249)

[52] (A autonomia da função de Encarregado de Proteção de Dados e a independencia do exercício da advocacia, 2018, p. 33)

opções tomadas por si no exercício de outras funções. O EPD deverá ser visto como um garante da proteção de dados em cada instituição, e não poderá ser responsável na determinação, aplicação ou efetivação de tratamentos ou meios de tratamento, se o for haverá conflito de interesses (cf. n.º 6 do artigo 38º do RGPD e Orientações do GT art. 29º sobre os EPD)[53].

É importante ter também em atenção o conteúdo da alínea b) do artigo 11.º da Lei n.º 58/2019 sobre as funções do Encarregado de Proteção de Dados, "*Sensibilizar os utilizadores para a importância da deteção atempada de incidentes de segurança e para a necessidade de informar imediatamente o responsável pela segurança;*" [sublinhado nosso], na qual parece haver o intuito do legislador em firmar que as questões de gestão relacionadas com os incidentes de segurança, deem ou não origem a violações de dados pessoais, são da competência do responsável de segurança. Importante notar que apesar de ser função do EPD a sensibilização dos utilizadores, é o responsável de segurança que deve ser alertado e não o EPD, pois será o responsável de segurança que tem a responsabilidade sobre a averiguação e resolução do possível incidente de segurança. No entanto é recomendado que as entidades consultem imediatamente o EPD após a ocorrência de uma violação de dados ou outro incidente[54], pois deverá o EPD apoiar na análise e possíveis impactos para os direitos, liberdades e garantias das pessoas singulares, decorrentes do incidente, emitindo parecer e orientações só no que a esses princípios diz respeito.

Neste aspeto, e salvaguardando a necessidade do EPD ser consultado após a ocorrência de um incidente de segurança, importa também salvaguardar que o EPD só poderá emitir parecer ou orientações sobre um determinado tratamento de dados, se dele tiver conhecimento[55].

"*O EPD não pode, pois, ter uma posição na organização que implique que seja ele a decidir as finalidades e os meios de tratamento de dados. Nessa área, para além de óbvias incompatibilidades (p. ex.: IT ou marketing) podem existir outras menos óbvias, mas também incompatíveis (p. ex.: serviços jurídicos).*"[56]
Da mesma forma ao EPD não cabe, controlar a realização de AIPD. Outro entendimento conduziria a que o EPD tivesse de emitir um parecer sobre um projeto que ele próprio elaborou, o que redundaria num inevitável conflito de interesses, contrário ao estatuto de independência que lhe é reservado[57].

Assim temos dois regimes a impor a nomeação de recursos

[53] (Orientações sobre os Encarregados da Proteção de Dados (EPD), 2017, p. 19)
[54] (Orientações sobre os Encarregados da Proteção de Dados (EPD), 2017, p. 16)
[55] "*Daqui decorre que, se não tiver sido informado de um tratamento de dados, também não pode informar a AEPD e, portanto, não pode cumprir eficazmente a missão essencial de supervisão que lhe é atribuída pelo legislador europeu*" (Athanassios Oikonomopoulos contra Comissão Europeia, 2016)
[56] (Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, 2021, p. 298)
[57] (O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas, 2020, p. 55)

humanos onde a necessidade de controlo de conformidade e de comunicação, nos respetivos âmbitos, parece ser um denominador comum. Em ambos os regimes, e esta imposição a todos os organismos da AP [58], vem mais uma vez demonstrar a importância e preocupação do legislador para com a segurança da informação tratada nas diversas entidades, assim como com o impacto que possa haver nos direitos, liberdades e garantias das pessoas singulares, decorrente de incidentes que comprometam algum tipo de informação. A importância das orientações do EPD torna-se relevante quando as mesmas devem refletir o foco nas pessoas singulares e apoiando o responsável de segurança, tudo fazer para ser ouvido sobre a gestão das medidas necessárias à segurança e demonstração da mesma.

No final, resta dizer que o EPD é um órgão consultivo sem poder de decisão nos aspetos relevantes ao tratamento de dados, pelo contrário, o responsável de segurança deverá ser capaz de determinar a forma e os meios como a informação deve ser tratada (onde se inclui dados pessoais), e até qual a informação relevante a monitorizar e registar para assim o comprovar.

5 Conclusões

No capítulo IV do RGPD epigrafado por "*Responsável pelo Tratamento e Subcontratante – Segurança dos dados pessoais*", encontramos aquilo que diretamente serão as responsabilidades do RT, e que vai desde o artigo 24.º "*Responsabilidade do responsável pelo tratamento*" até ao artigo 43.º "*Organismos de certificação*". Importa no âmbito deste trabalho alavancar a necessidade do legislador em colocar neste capítulo o artigo 25.º "*Proteção de dados desde a conceção e por defeito*", artigo 32.º "*Segurança do Tratamento"*, artigo 35.º "*Avaliação de impacto sobre a proteção de dados*", artigo 37.º "*Designação do encarregado da proteção de dados*" e artigo 39.º "*Funções do encarregado da proteção de dados*", dando a indicação direta que estes assuntos são da responsabilidade do RT.

Não é possível garantir o direito à privacidade e à proteção dos dados pessoais sem aplicar todas as medidas técnicas e organizativas (cf. n.º 1 do artigo 24º do RGPD), no que respeita à segurança da informação. Teremos sempre de considerar que dados pessoais são uma categoria especial de informação que deverá ser protegida mediante os riscos apresentados (cf. n.º 1 e n.º 2 do artigo 32º do RGPD, considerados 83, 74, 75, 76 e 77).

No que respeita à Segurança da Informação, Confidencialidade, Integridade e Disponibilidade, esta só é possível aplicando, com base na gestão de risco e AIPD, todas as medidas necessárias à segurança das redes e sistemas onde esta informação é tratada, transmitida, armazenada, e dir-se-ia que até mesmo eliminada. A eliminação não deixa de ser um tratamento tanto ou mais importante que os outros, e convém ser efetivado com a maior das garantias de eficácia e segurança.

[58] Com a exceção identificada na segunda parte da alínea a) do n.º 1 do artigo 37.º do RGPD

A base da garantia da informação e proteção de dados, é a efetivação real de análises de risco inseridas num sistema de gestão de risco e que permitam aferir mediante o valor dos ativos, vulnerabilidades conhecidas e possíveis ameaças quais as medidas necessárias para eliminar, mitigar ou até se necessário transferir os riscos identificados. No tratamento correto do risco, estar-se-á a responder à parte técnica da AIPD no garante dos direitos das pessoas singulares, sendo assim, uma análise de risco de acordo com o solicitado quer no Decreto-Lei n.º 65/2021 como no Regulamento 303/2019, não é uma AIPD, mas na verdade, parte da mesma.

A responsabilidade do EPD quanto à segurança, só está no dever de orientar o RT sobre a necessidade de aplicar medidas técnicas e organizativas na segurança dos dados pessoais, mas nunca na determinação das mesmas, até porque a determinação de controlos na sua grande maioria implica determinar tratamento de dados pessoais, que cabe ao EPD monitorizar a conformidade, desta forma não parece possível acumular a função de EPD com a de responsável de segurança.

Assim verifica-se que o Decreto-Lei n.º 65/2021 e o Regulamento n.º 303/2019 vêm ajudar no trabalho necessário à garantia da informação e proteção de dados pessoais, pois estabelecem nas organizações dentro do seu âmbito de aplicação, uma série de medidas que por sua vez melhoram o trabalho necessário na conformidade com o RGPD, Lei n.º 58/2019 e Lei n.º 41/2004.

Importante perceber que em termos de legislação sobre a matéria de segurança de redes e serviços de informação, a Lei das Comunicações Eletrónicas, Lei n.º 5/2004 na sua versão atual, estabelecia uma igual preocupação no que respeita aos serviços de comunicações eletrónicas e seus prestadores, nomeadamente no artigo 54.º-A "*Obrigações das empresas em matéria de segurança e integridade*", artigo 54º-B "*Obrigações de Notificação*", e no artigo 54.º-C "*Medidas de execução*". Esta operacionalização fica a cargo da ANACOM que o faz através do Regulamento n.º 303/2019, que impõe a comunicação de contato permanente, responsável de segurança, envio de relatório anual, análises de risco, plano de segurança e obrigações de notificação das violações de segurança, de igual forma com o agora Decreto-Lei n.º 65/2021 que operacionaliza a Lei n.º 46/2018.

Existirão inclusive entidades que, prestando serviços de telecomunicações nos termos da Lei n.º 5/2004, prestarão serviços digitais identificados no Anexo da Lei n.º 46/2018, e que assim terão obrigações de identificação, elaboração e reporte sobre segurança da informação e proteção de dados para três Autoridades distintas, a saber: CNPD, CNCS e ANACOM.

No final, é da máxima importância que as entidades devam "*assumir que nunca estão seguras e não podem confiar que o cumprimento da lei as exime de qualquer responsabilidade, tendo de ter, também, em linha de conta que os processos legislativos tendem a ser mais lentos*

que a evolução tecnológica"[59]. É importante ter a consciência que quanto a ataques, incidentes de segurança e violação de dados, não se coloca a questão se irão acontecer, mas sim, quando é que irão acontecer.

Nesse sentido, na aplicação das medidas de segurança e Cibersegurança, quer as estabelecidas na legislação de Cibersegurança em apreço, como outras emanadas das diversas normas [60] internacionais, deverá ser dado também atenção às medidas reativas e de recuperação que permitam a continuidade do negócio, pelo que nos planos de segurança previstos no artigo 7.º do Decreto-Lei n.º 65/2021 é importante contemplar as medidas de recuperação de eventuais incidentes de segurança com ou sem violação de dados pessoais.

Conclui-se então que aplicar a legislação existente no que concerne à Cibersegurança e segurança da informação com caráter regulado e sancionatório, irá permitir alavancar as medidas necessárias na proteção de dados. Torna-se então necessário tirar partido destas medidas no ponto de vista da proteção de dados, e perceber que haverá espaço para a atuação das diversas autoridades de controlo na medida de complementaridade. Neste aspeto é importante salientar que deverá fazer parte da documentação respeitante à segurança da informação e proteção de dados a notória separação de competências e procedimentos, até porque em determinados pontos parecem sobrepor-se, como seja por exemplo o caso do registo de incidentes e do registo de violações de dados.

Bibliografia

Alves, D. L. (2021). O papel fundamental da Cibersegurança na Proteção de Dados Pessoais. *in Anuário da Proteção de Dados*, 121-154.

Amorim, A. (21 de 10 de 2021). *Onde fica o DPO dentro das Empresas*. Obtido de Security Report: https://www.securityreport.com.br/colunas-blogs/onde-fica-o-dpo-dentro-das-empresas/#.YXu9rF7PyUk

Andrade, R. R. (2020). Da responsabilidade do Encarregado de Proteção de Dados. *in Forum da Proteção de Dados*, 24-43.

Athanassios Oikonomopoulos contra Comissão Europeia, Processo T-483/13, ECLI:EU:T:2016:421, n.º 100 (Tribunal Geral (Quarta Secção) 20 de julho de 2016).

Centro Nacional de Cibersegurança. (2019). Quadro Nacional de Referência para a CiberSegurança. Lisboa.

Cordeiro, A. B. (2018). A autonomia da função de Encarregado de Proteção de Dados e a independencia do exercício da advocacia. *in Revista da Ordem do Advogados*, 17-38.

Cordeiro, A. B. (2020). *Direito da Proteção de Dados*. Coimbra: Edições Almedina.

[59] (O papel fundamental da Cibersegurança na Proteção de Dados Pessoais, 2021, p. 134)

[60] Diretiva (UE) 2016/1148, n.º 11 do artigo 4.º "*«Norma», uma norma na aceção do artigo 2.o, ponto 1, do Regulamento (UE) n.º 1025/2012;*"

Cordeiro, A. B. (2021). *Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019*. Coimbra: Edições Almedina.

ECIIA and FERMA. (21 de 9 de 2010). Guidance on the 8th EU Company Law Directive - Directive 2006/43/EC – Art. 41-2b. *Monitoring the effectiveness of internal control, internal audit and risk management systems*.

Fernanda Maças, Filipa Galvão. (2020). O Encarregado de Proteção de Dados nas Pessoas Coletivas Públicas. *Forum de Proteção de Dados*, 44-62.

Filipa Galvão. (2018). Parecer à Proposta de Lei n.º 120/XIII/3.ª Gov. *PARECER N.º 20/2018 - Processo n.º 6275/2018*. Lisboa: CNPD.

Freitas, V. (29 de 9 de 2021). *Ciberlaw Publicação - A Regulação Juridica do Ciberespaço - Mutação do paradigma à luz do Acórdão James Elliot do TJUE*. Obtido de Centro de Investigação Jurídica do Ciberespaço: https://www.cijic.org/wp-content/uploads/2020/04/IV_A-Regulacao-juridica-do-ciberespacao_mutacao-do-paradigma-a-luz-do-Acordao-James-Elliot-do-TJUE_Valter-Freitas.pdf

Grupo de Trabalho do Artigo 29.º para A proteção de Dados. (04 de abril de 2017). 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. *WP248rev.01*. Comissão Europeia.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (5 de abril de 2017). Orientações sobre os Encarregados da Proteção de Dados (EPD). *WP243rev.01*. Comissão Europeia.

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (06 de fevereiro de 2018). Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679. *WP250rev.01*. Comissão Europeia.

International Standard Organization. (junho de 2017). ISO/IEC 29134:2017. *Information technology — Security techniques — Guidelines for privacy impact assessment*. Geneva: ISO/IEC.

International Standard Organization. (2018). ISO/IEC 27005:2018. *Information technology — Security techniques — Information security risk management*. Geneva: ISO/IEC.

International Standard Organization. (agosto de 2019). ISO/IEC 27701:2019. *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. ISO/IEC.

La Commission Nationale de l'Informatique et des Libertés. (16 de novembro de 2021). Guide Pratique RGPD, Délégués à la protection des données. CNIL.

Martins, J. C. (2021). *Gestão de Segurança e Cibersegurança nas Organizações*. Faro: Silabas & Desafios.

Pica, L. (21 de 10 de 2021). *CiberLay - As AIPD, o EPD e a Certificação no novo RGPD*. Obtido de Centro de Investigação Jurídica do Ciberespaço: https://www.cijic.org/wp-content/uploads/2018/03/3_AS-AVALIA%C3%87%C3%95ES-DE-

IMPACTO-O-ENCARREGADO-DE-DADOS-PESSOAIS-E-A-CERTIFICA%C3%87%C3%83O-NO-NOVO-REGULAMENTO-EUROPEU-DE-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf

Saldanha, N. (2018). *Novo Regulamento Geral de Proteção de Dados. O que é? Aquem se aplica? Como implementar?* Lisboa: FCA Editora.

The European Data Protection Supervisor. (6.6.2009). Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC. *Official Journal of the European Union C 128*, 28-41.

JAVALI
OPEN SOURCE SYSTEMS

A solução web à medida do seu negócio

+ 20 anos experiência

+ 300 clientes satisfeitos

+ 10 setores de atividade

+ 300 projetos desenvolvidos

Serviços e soluções para projetos de sucesso

- Consultoria
- Gestão de Projeto
- Web Design
- Desenvolvimento web - Drupal
- Formação
- Suporte pós-produção
- Manutenção
- Websites
- Intranets
- Lojas online
- Plataformas para Instituições de Ensino
- Plataforma para Rent-a-Car
- Desenvolvimento à medida

MINISTÉRIO PÚBLICO
PORTUGAL

"Vimos por este meio expressar o gosto que tivemos em trabalhar com a Javali, foi extremamente gratificante, em grande parte pela sintonia e perfeita colaboração com a PGR, mas também, e sobretudo, pela extrema simpatia da vossa equipa, disponibilidade, profissionalismo e competência."

Nelson Coelho e Cândida Ferreira, Procuradoria-Geral da República

CASCAIS
Tudo começa nas pessoas

"Quando a Câmara Municipal de Cascais apostou na criação do seu novo portal, a Javali foi a empresa escolhida para a sua implementação. De lá para cá têm sido nossos parceiros na manutenção técnica e evolutiva do portal, dando resposta na íntegra às necessidades de um projeto que sabemos inovador e criativo."

Matilde Cardoso, Câmara Municipal de Cascais

REPÚBLICA PORTUGUESA
DEFESA NACIONAL

BANCO DE PORTUGAL
EUROSISTEMA

Secretaria-Geral da Educação e Ciência

DGES
Direção-Geral do Ensino Superior

UCCLA

GRUPO Manuel Champalimaud

sumol+compal
É da nossa natureza.

omi

Ispa

NOVA
FACULDADE DE CIÊNCIAS E TECNOLOGIA

NICE RENT

Oliveira Seguros

esop

Contacte-nos

(+351) 212 957 215 | info@javali.pt | www.javali.pt

Responsáveis conjuntos pelo tratamento – quem determina o quê?

Fernanda Fragoso

Encarregada de Proteção de Dados

Santa Casa da Misericórdia de Lisboa

O artigo 4º/7), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, (Regulamento Geral sobre a Proteção de Dados – RGPD), define como "Responsável pelo tratamento, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individual ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro."

Nesta definição, destaca-se que o responsável pelo tratamento ao determinar as finalidades e os meios de tratamento dos dados pessoais, pode fazê-lo em conjunto com outros.

Com o RGPD, é introduzida a norma do artigo 26º que vem clarificar os requisitos da responsabilidade conjunta.

Artigo 26º

Responsáveis conjuntos pelo tratamento

"1. Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as

informações referidas nos artigos 13.º e 14.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados.

2. O acordo a que se refere o n.º 1 reflete devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. A essência do acordo é disponibilizada ao titular dos dados.

3. Independentemente dos termos do acordo a que se refere o n.º 1, o titular dos dados pode exercer os direitos que lhe confere o presente regulamento em relação e cada um dos responsáveis pelo tratamento."

A aparente simplicidade na determinação dos conceitos plasmados nos artigos 4º/7) e 26º, nº1, primeira parte, do RGPD, traduz, paradoxalmente, uma elevada complexidade na exequibilidade da responsabilidade conjunta pelo tratamento dos dados pessoais. Quem determina o quê?

Para identificar as diferentes obrigações impostas aos responsáveis conjuntos pelos tratamentos, perante os titulares dos dados, é preciso ter sempre presente os princípios da licitude, lealdade e transparência, enunciados no artigo 5º, nº1, alínea a), do RGPD, de forma a não defraudar a "accountability" com a prestação de contas que o responsável pelo tratamento tem de prestar aos titulares dos dados pessoais (artigo 5º, nº2, do RGPD).

Pela importância do enquadramento histórico da terminologia, o Parecer do Grupo de Trabalho do Artigo 29º / WP 169 (págs. 6 e 7) refere, quanto ao texto original da Convenção 108:

"(...) o termo «responsável pelo ficheiro» constante da Convenção n.º 108 foi substituído pelo termo «responsável pelo tratamento» de dados pessoais. O termo «tratamento de dados pessoais» é um conceito muito vasto, sendo definido no artigo 2.º, alínea b), da Directiva como «qualquer operação ou conjunto de operações efectuadas sobre tratamento de dados pessoais, com ou sem meios automatizados, tais como a recolha, registo, organização, conservação, adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, o apagamento ou a destruição.». Assim, o conceito de «responsável» deixou de ser utilizado por referência a um objecto estático («o ficheiro»), sendo antes associado a actividades que reflectem o ciclo de vida da informação, desde a sua recolha à sua destruição, o que exigia uma análise pormenorizada e global («operação ou conjunto de operações»). Embora o resultado possa ter sido o mesmo em muitos casos, foi atribuído ao conceito um significado e um âmbito muito mais vastos e dinâmicos.

Outras alterações envolviam a previsão da possibilidade de «controlo colectivo» («individualmente ou em conjunto com outrem»), o requisito de que o responsável

pelo tratamento «determine as finalidades e os meios de tratamento dos dados pessoais» e a ideia de que esta determinação pode ser efectuada pela legislação nacional ou comunitária ou de outra forma. A Directiva introduziu também o conceito de «subcontratante», que não é mencionado na Convenção 108. (…)

Deste modo, o principal papel do conceito de responsável pelo tratamento é, antes de mais, determinar quem será o responsável pelo cumprimento das normas sobre protecção de dados e de que modo as pessoas em causa podem exercer na prática os seus direitos. Por outras palavras: atribuir a responsabilidade."

Na 128ª Sessão, de 18 de maio de 2018, o Conselho de Ministros, do Conselho da Europa tomou em consideração o Parecer nº 296 (2017) da Assembleia Parlamentar sobre o Protocolo de emenda à Convenção para a Proteção das pessoas em relação ao tratamento automatizado de dados pessoais e adotou o referido Protocolo realçando a importância de uma adesão rápida, pelo maior número possível de Estados atualmente Partes da Convenção nº 108, deliberando abrir à assinatura dos mesmos o texto da Convenção 108 modernizada, conducente à ratificação, aprovação ou aceitação do referido Protocolo, que formalizará a vinculação dos respetivos signatários às obrigações decorrentes da Convenção alterada / Convenção 108 +

Assim, o artigo 2º, alínea b), da Convenção 108 modernizada, define como "responsável pelo tratamento "a pessoa física ou moral, autoridade pública, serviço, agência ou qualquer outro órgão que, por si só, ou em conjunto com outros, tem o poder de decisão relativo ao tratamento de dados;"

Como é sublinhado no *Manuale sul diritto europeu in materia di protezione dei dati* (ed.2018 – págs. 114 a 121), "Os particulares quando tratam dados de terceiros no contexto de atividades de natureza exclusivamente pessoal ou doméstica, não se enquadram no âmbito de aplicação das regras do RGPD e da Convenção 108 modernizada, e não são considerados responsáveis pelo tratamento de dados."

Pelo contrário, "as regras de proteção de dados aplicam-se integralmente aos responsáveis pelo tratamento e aos subcontratantes que fornecem os meios para processar dados pessoais no âmbito da atividade, no contexto de atividades pessoais ou domésticas (como por exemplo, as plataformas de redes sociais). (…)

O RGPD estabelece que quando dois ou mais responsáveis pelo tratamento determinam conjuntamente as finalidades e os meios do tratamento, são responsáveis conjuntos pelo tratamento. isto significa que decidem em conjunto tratar os dados para uma finalidade comum. A Convenção 108 modernizada também prevê a possibilidade de múltiplos responsáveis pelo tratamento ou co-controladores de dados, no âmbito do Conselho da Europa."

Já com o Parecer nº1/2010 sobre os conceitos de "responsável pelo tratamento" e "subcontratante", produzido pelo Grupo de

Trabalho do Artigo 29ª – WP169, encontramos diversos exemplos ilustrativos da grande complexidade decorrente do processamento dos dados, em particular, quanto à participação de diferentes responsáveis pelo tratamento dos dados e com diversas formas de controlo com as atividades desse tratamento.

Sumariamente, os requisitos determinantes para aferirmos o responsável pelo tratamento e, em particular, os responsáveis conjuntos pelo tratamento, em sintonia com o Parecer WP 169 são:

- a autonomia do responsável pelo tratamento para estar em conformidade com a legislação da UE em matéria de proteção de dados, bem como o carácter funcional entendido como aquele que determina "de facto" as finalidades e os meios desse tratamento;

- o carácter funcional assegura o controlo das atividades de tratamento, daí a responsabilização na "prestação de contas" (*accoutability*) decorrente do princípio da responsabilidade proativa, constante no artigo 5º, nº2, do RGPD;

- para isso, o responsável pelo tratamento tem de comprovar que observou os princípios relativos ao tratamento de dados pessoais, constantes no nº1, do artigo 5º, do RGPD.

Quando o tratamento de dados pessoais é efetuado, em conjunto, por dois um mais responsáveis, é necessário acordar entre eles, quando determinam as finalidades e os meios do tratamento, quais as responsabilidades atribuídas a cada um e, consequentemente, quem é o responsável por aquele tratamento específico que impacta com os direitos e liberdades dos titulares dos dados!

O princípio da transparência impõe aos responsáveis pelo tratamento a obrigação de informar os titulares dos dados sobre o impacto do tratamento!

Esta responsabilidade pode desenvolver-se de diferentes níveis no decurso do tratamento. Daí o artigo 26º, nºs1 e 2, do RGPD, exigir que os responsáveis conjuntos pelo tratamento, estabeleçam, formalmente, um acordo entre si, de forma clara e transparente, assinalando as responsabilidades que lhes competem, em matéria de conformidade, disponibilizando-o aos titulares dos dados, e acautelando, especificamente, qual, ou quais, dos responsáveis conjuntos pelo tratamento responde, em cada momento, perante os titulares dos dados para dar resposta ao exercício dos respetivos direitos.

Não obstante a formalização do acordo de parceria haverá sempre responsabilidade solidária, por parte dos responsáveis conjuntos pelo tratamento, face aos titulares dos dados.

No citado, *Manuale sul diritto europeu in materia di protezione dei dati*, refere-se que "a contitularidade determina a responsabilidade conjunta por uma atividade de tratamento. No contexto do direito da UE, isto significa que cada responsável pelo tratamento ou subcontratante pode ser responsabilizado solidariamente pelo montante total dos danos

causados pelo tratamento conjunto, a fim de garantir uma compensação efetiva dos interessados" (…) e continua mencionando que "O Grupo de Trabalho do Artigo 29º, estabelece que os responsáveis conjuntos pelo tratamento podem partilhar todas as finalidades e todas as ferramentas de um tratamento, algumas finalidades ou meios, ou parte deles. Enquanto no primeiro caso as relações entre os diferentes intervenientes seriam muito próximas, no segundo caso seriam mais distantes. O Grupo de Trabalho do artigo 29.º inclina-se para uma interpretação mais ampla do conceito de responsabilidade conjunta, a fim de permitir uma certa flexibilidade que tenha em conta a crescente complexidade do atual tratamento de dados pessoais." (tradução livre).

No Parecer do Grupo de Trabalho do Artigo 29º / WP 169, é referido o **caso SWIFT**, que envolveu a Sociedade de Telecomunicações Financeiras Interbancárias Mundiais, para exemplificar uma situação de controlo decorrente de uma influência de facto e não meramente formal.

Assim, "o próprio facto de uma entidade determinar o modo como os dados pessoais são tratados poderá implicar a sua qualificação como responsável pelo tratamento, ainda que esta qualificação não resulte de uma relação contratual ou seja expressamente excluída por um contrato. Esta situação é claramente ilustrada pelo caso SWIFT, em que esta empresa decidiu, na sequência de intimações emitidas pelo Departamento do Tesouro dos Estados Unidos, facultar a esta entidade o acesso a determinados dados pessoais – originalmente tratados para fins comerciais por conta de instituições financeiras – para fins de combate ao financiamento do terrorismo." (…)

"(…) o termo «meios» não abrange apenas os meios técnicos de tratamento dos dados pessoais, mas também o modo de tratamento, que implica a resposta a perguntas como «que dados serão tratados», «que terceiros terão acesso a estes dados», «quando é que os dados serão eliminados», etc." (…)

"Em geral, a análise do controlo conjunto deve ser semelhante à análise do controlo

«individual» (…) Da mesma forma, também a análise do controlo conjunto se deve basear numa abordagem substantiva e funcional, tal como ilustrado anteriormente, centrada na identificação das entidades que determinam as finalidades e os meios de tratamento." (págs. 15, 18 e 23).

Conclui-se, realçando a necessidade para uma avaliação criteriosa do(s) objetivo(s) do tratamento, designadamente:

- quem é o responsável por determinar as finalidades e os meios do tratamento dos dados;
- se essa determinação envolveu, conjuntamente, mais do que um responsável pelo tratamento, para efeitos dos requisitos plasmados no artigo 26, nº1, do RGPD;
- quem detém o controlo funcional do tratamento.

Diferentemente, se no âmbito do tratamento de dados pessoais

verificarmos existir somente uma cooperação entre as várias entidades envolvidas no desenvolvimento de diversas atividades com objetivos diferentes, poderemos estar somente perante uma realidade de transferência de dados entre diferentes responsáveis pelo tratamento e não perante responsáveis conjuntos pelo tratamento!

Não podemos chegar tarde a ontem!

Sílvio Gomes

Sócio e gerente | Director de Projectos

Compliance Way

Sob a epígrafe "O papel da Proteção de Dados Pessoais na Inteligência Artificial" vai decorrer o V Encontro Nacional da APDPO.

Espera-se que em ambiente distendido, mas não menos preocupado, e com um painel de oradores que permite antever um elevado nível no tratamento do tema, um conjunto de "profissionais de protecção e de segurança dos dados" apreciem a importância crescente deste tema nas sociedades actuais, nas organizações, e também para si.

Não se quer mais um debate diletante sobre efabulações paradisíacas de um futuro que se anuncie. Também não se quer um fórum de "cientistas" com inúmeras teorias preditivas. Menos ainda um absurdo confronto de ideias que oponham os homens e as máquinas.

Aguarda-se uma abordagem holística e equilibrada, entre as venturas e as desventuras tecnológicas, a significância do perfil ético das finalidades e dos meios, o estado da arte da regulação, os impactos positivos inegáveis, e as ainda desconhecidas consequências negativas para os cidadãos.

Pela importância e actualidade do tema, espera-se que não esfrie após o V Encontro, e que se amplifiquem os ecos da necessidade imperiosa em deslocar-se o debate actual, muito enviesado e focado nos benefícios das maravilhas tecnológicas dos modelos de inteligência artificial (IA), para o centrar na dimensão humana da vida.

Não podemos ignorar

A tendência nas organizações é para planearem a incorporação dos modelos de IA mais adequados aos processos de decisão, de

negócio, e de suporte, para uma diferenciação no mercado, e pela geração máxima de valor, como o bem único e supremo.

Não podemos ignorar a "magia" da vorticidade da perda da titularidade dos dados.

A opacidade tecnológica, em especial da alma algorítmica, bem como o desfasamento crescente entre a evolução exponencial da complexidade dos modelos de IA, e a aquisição aritmética e lenta do conhecimento sobre os impactos desses modelos, dificulta o propósito dos encarregados da protecção de dados (EPD), mas convoca-os para abraçarem os novos desafios para o pleno exercício do seu cargo.

Os novos desafios que se colocam às organizações que adoptam modelos de IA, quanto à conformidade legal, à responsabilidade demonstrável, à segurança da informação e do tratamento de dados, e à responsabilidade social, são imensos e encerram enigmas.

Cumulativamente, e nas organizações cuja maturidade permite o desenvolvimento do negócio em conformidade com o regime jurídico da protecção de dados, ainda subsistem muitas dúvidas sobre aspectos mais "comezinhos" da gestão da protecção de dados, que também não são alheias ao cargo de EPD. A título de exemplo, considere-se a classificação do estatuto jurídico das organizações parceiras pela função que exercem no tratamento dos dados, a gestão dos riscos para os titulares, o preenchimento e conservação actualizada do registo das actividades de tratamento, a AIPD, entre outras obrigações.

A maioria dos órgãos dirigentes das organizações, e à margem da responsabilidade legal no tratamento dos dados pessoais, não têm a preocupação de assegurar um modelo de governo da transformação para a transição digital assente no compromisso entre os interesses do negócio, e o dever de conformidade quanto aos dados pessoais dos titulares. Sabem que estes lá vão depositando os seus dados pessoais, à sua guarda, no mais completo desconhecimento sobre o modo discricionário como essa "matéria-prima" grátis é usada, muito longe da protecção exigida por um direito fundamental.

A incorporação de tecnologias novas nas organizações, acrescenta obrigações para a completude do cumprimento dos princípios, da licitude do tratamento, da ponderação da necessidade e proporcionalidade dos meios empregues, desde a concepção e por defeito, da adopção de novas medidas técnicas e organizativas, da informação a facultar aos titulares para o conhecimento, o controlo e o exercício dos seus direitos, do registo das actividades de tratamento, da AIPD, etc.

Um tsunami seco

Os EPD não podem alhear-se do tsunami seco que as tecnologias estão a provocar na privacidade dos titulares, na protecção dos seus dados, e no exercício do cargo.

Os titulares, sem acesso às informações que lhes são devidas, e de acordo com as regras

estabelecidas, continuam desprotegidos e facilmente desvalorizam e entregam o ouro que desconhecem ter.

Esta vulnerabilidade alimenta muita investigação e desenvolvimento dos modelos de IA, que conta com o ritmo lento e tardio da regulação, e com a cumplicidade de alguns Estados e autoridades de controlo. O caminho está livre, e teme-se que assim continue.

Pela incorporação acrescida das tecnologias nos processos organizacionais, em especial dos modelos de IA aplicados à gestão do negócio, dos mercados, dos clientes e dos trabalhadores parece inevitável que os EPD tenham de adquirir níveis superiores de literacia digital sobre o "boost" que esses modelos trazem à operacionalização das actividades de tratamento de dados.

A gestão do risco, por concepção e por defeito, em conformidade com a Avaliação do Impacto da Protecção de Dados (AIPD) também deve reflectir esta nova realidade. Aumenta o âmbito e a complexidade dos pressupostos a apreciar para se estabelecerem novas medidas adequadas aos novos meios de tratamento.

Novas competências

Para o exercício do cargo de EPD, é cada vez mais necessário ganhar novas qualificações, enquanto competências demonstradas, ou seja, aptidão para aplicar novos conhecimentos e saber-fazer para atingir os resultados pretendidos para a conformidade das organizações.

Sem novas competências não pode falar-se de acompanhamento e aconselhamento no tratamento dos dados, na apreciação ao risco, na implementação das medidas de segurança adequadas, nas acções de sensibilização e formação, de auditoria, etc.

Existe o risco do exercício do cargo de EPD se esfumar na formalidade cómoda de um papel inócuo, longe de uma comparticipação consultiva substancial.

Quanto às auditorias, internas ou externas, programadas ou não programadas (preferencialmente), entende-se que o EPD, apesar de não ter autoridade decisória para assegurar a sua realização, deve incorporá-las no seu plano anual de actividades e no relatório para a Alta Direcção, onde aprecia o real estado de maturidade na materialização da conformidade comprovável.

Ainda sobre as auditorias, deve realçar-se que só com as evidências aí recolhidas, expressas em constatações que sugerem recomendações, podem ultrapassar-se muitas resistências organizacionais "surdas", sob cortinas nebulosas, cheias de cosmética em narrativa, que alimentam mitos e crenças na conformidade das organizações, sem a noção exacta das vestes que continuam a faltar ao Rei!

Concorda-se que, para além das qualidades profissionais do EPD, se considere que têm de ter "conhecimentos especializados no domínio do direito", o que assegura, em última instância, a certeza jurídica da conformidade dos tratamentos de dados. Mas não é

menos verdade que essa certeza pode desvanecer-se, senão mesmo esvair-se com a magia tecnológica.

Com alguma boa vontade, pode antecipar-se que o legislador, por prever esse cenário, tenha acrescentado a valência lógica "das práticas de protecção de dados". Admitindo-se que no saco "das práticas" se possa ler uma sugestão sublime ao perfil tecnológico, não pode deixar de registar-se a falta de uma referência explícita e robusta, em linha com a importância que o RGPD dedica às "tecnologias mais avançadas".

Mesmo que o recurso a equipas pluridisciplinares, de apoio ao EPD, ajude a colmatar "algumas faltas", não se resolve a insuficiência das competências críticas para assegurar a autonomia de análise e decisão consultiva do EPD no seio da organização, e da sua própria equipa de apoio.

Já emergiu!

O tempo urge. O desenvolvimento dos modelos de IA, a disseminação por produtos e serviços à escala do mercado mundial, coexistem com as mais elementares tarefas diárias, e estilos de vida dos cidadãos, quantas vezes de modo imperceptível.

Os modelos de IA sucedem-se a um ritmo vertiginoso, e já passou a idade de tecnologia emergente. Já emergiu, e com um catálogo denso de modelos, desde os de uso proibido (que los hay, los hay!), aos de alto risco, até aos considerados "aceitáveis".

Se as anteriores revoluções tecnológicas foram moldando aspectos da vida humana, os modelos de IA tendem a mudar o próprio significado do ser humano.

De um modo geral, assiste-se ao franco desenvolvimento das inovações maravilhosas para a vida natural, em um estonteante alargamento das suas descobertas a todas as áreas da organização social, como sejam, o mundo do trabalho e as novas competências, a saúde, o ensino, a financeira, a seguradora, a mobilidade, a justiça, a prevenção e a investigação criminal, o governo das organizações, a gestão do risco, a modelação dos processos de negócio e de suporte, etc.

A IA impõe-se como mais um contributo magnífico da inteligência natural para a história do pensamento humano.

Criada pelo criador

Nos meios da investigação e desenvolvimento dos modelos de IA, profetiza-se que, dentro de uma década, ganhem novas dimensões intuitivas e emocionais, ainda que, sob a fatalidade da artificialidade, a sua inteligência continue sem ter vida natural própria.

A sua alma é conferida pelo "criador" para este prosseguir com novas criações, sejam elas o que forem.

Todos os modelos de IA têm a inteligência humana como eixo do movimento helicoidal em que se desenvolvem, à qual, por sua vez, disponibilizam infindáveis potencialidades para uma evolução incessante, ora incremental ora disruptiva.

Também se profetiza que, dentro do mesmo período temporal

de dez anos, possa verificar-se a passagem da fase de prototipagem da computação quântica, para o seu advento no mercado, ainda que limitado a alguns Estados e a algumas empresas, o que não deixa de ser mais um elemento perturbador do desigual desenvolvimento, com a discriminação no lugar da tão almejada harmonia e promessas de democraticidade.

Pela superior capacidade e velocidade dos "qubits" no processamento de dados, e a combinação com novos modelos de IA, não é difícil imaginar um novo salto, uma verdadeira disrupção "mesmo disruptiva", nas tecnologias de informação e comunicação, nas redes e dispositivos. Admite-se mesmo que os impactos nos pressupostos da segurança da informação e da cibersegurança, que hoje conhecemos, continuem algo insondáveis.

O que nos tranquiliza é saber que, em paralelo, estão em estudo novos pressupostos para conferir um estado superior de segurança e resiliência, para enfrentar a onda de desafios disruptivos, a que não escaparemos.

Não nos iludamos. É tão absurdo querer parar o vento e as intempéries da IA com as mãos, quanto expormo-nos ao vendaval sem avaliar o limite da aceitabilidade, sem apreciar os riscos associados, e as consequências para a vida humana, demitindo-nos de exigir uma regulação e fiscalização efectivas, e não uma barquinha que "lá vem, lá vem"!

* O artigo está escrito em harmonia com o antigo acordo ortográfico.

COMPLIANCE WAY®

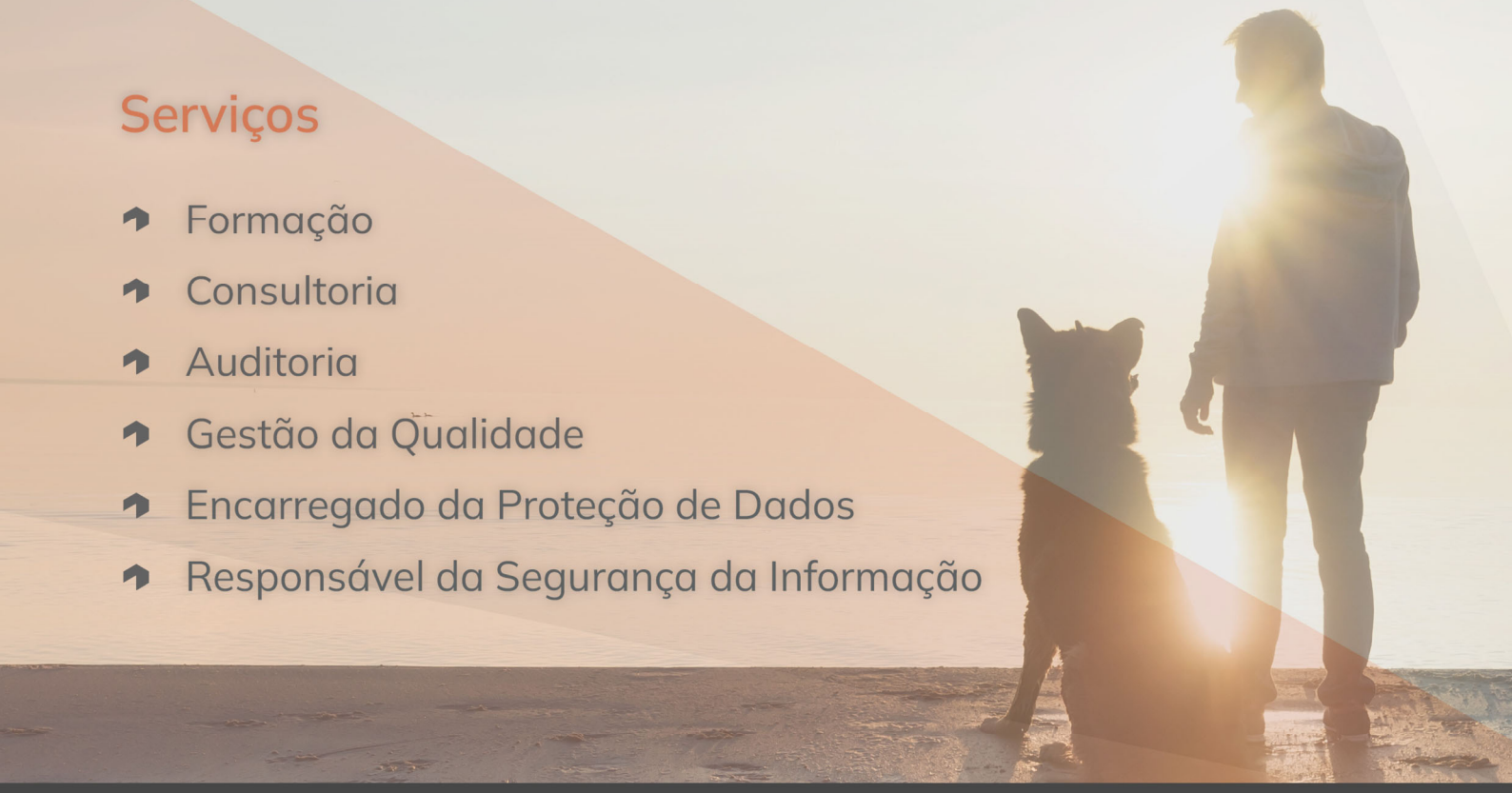
Conformidade | Competência | Confiança

Áreas de Competência

- Qualidade | Implementação
Gestão de Sistemas
- Proteção de dados | Adequação das Organizações ao RGPD
Implementação do Processo de Gestão
- Segurança da Informação e Cibersegurança
- Ciberseguros | Avaliação para a transferência dos riscos

Serviços

- Formação
- Consultoria
- Auditoria
- Gestão da Qualidade
- Encarregado da Proteção de Dados
- Responsável da Segurança da Informação



geral@complianceway.pt +351 910 510 361 www.complianceway.pt