
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VII – MAIO DE 2019

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antes de mais, aproveito para anunciar uma nova edição do Curso de Direito do Ciberespaço, em formato novel, a ter lugar em Novembro de 2019. À semelhança do curso anterior, na oportunidade de publicação de alguns artigos, a Revista assumir-se-á como esse veículo de partilha de conhecimento.

No que concerne propriamente às notas desta edição, permitam-me partilhar algumas novidades e preocupações.

No passado dia 23 de maio do corrente, o Conselho de Ministros aprovou a Estratégia Nacional de Segurança do Ciberespaço (ENSC) 2019-2023, que ainda carece de publicação em jornal oficial. Não obstante é já do domínio público que o propósito desta nova ENSC visará *garantir a proteção e a defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas, procedendo desta forma à revisão da ENSC de 2015*[1], tendo em atenção a evolução digital ocorrida desde então.

1 https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278
A propósito, neste conspecto, para quem não tenha estado presente, na Conferência – Cibersegurança, na Universidade de Évora, a 14 de novembro de 2018, será interessante dar uma vista de olhos na apresentação "A Estratégia Nacional de Segurança do Ciberespaço 2.0 – Governação e execução", feita e disponibilizada por parte do CALM Gameiro Marques, da Autoridade Nacional de Segurança, cujo conteúdo pode ser encontrado @ https://www.uevora.pt/media_informacoes/agenda/(item)/25903.

Em efeméride de aniversário do Regulamento Geral de protecção de dados, e estando este em vigor desde *o vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia*, naturalmente a «Cyberlaw by CIJIC» não poderia passar ao lado do tema, recorrente dos últimos anos.

De facto, nestes 3 anos volvidos, é inconcebível que Portugal ainda não tenha uma lei de execução do mesmo. De igual forma, é inconcebível que as organizações, públicas ou privadas, só conheçam o "consentimento" como fundamento de licitude para o tratamento de dados pessoais, considerando-o um verdadeiro *canivete-suíço*. Ainda havemos de pugnar por um "*direito ao esquecimento*" sobre o consentimento, pois que a livre revogabilidade do mesmo por parte da pessoa titular dos dados pessoais parece sucumbir ante tanto abuso na sua utilização por parte das mais variadas organizações.

Se a estupefação quanto ao uso abusivo da figura do consentimento não cercear a nossa incredulidade, é igualmente inconcebível que o Estado, hoje, 3 anos após a entrada em vigor do RGPD, tenha dado conta de que, por exemplo, pelo menos, 1977 freguesias estarão obrigadas a nomear um encarregado de protecção de dados. Subam ou desçam na hierarquia do Estado e imaginem a confusão em que se vive. Três anos volvidos e o Mercado Único Digital Europeu à espreita…

Não pensem, contudo que a confusão é exclusivo do sector público. Quando o foco deriva para dados pessoais sensíveis, nomeadamente, dados de saúde, notícias como por exemplo, «*Proteção de Dados condena clínicas que recusam tratar doentes por falta de assinaturas*[2]», revelam parte do preocupante e actual estado de coisas.

Com efeito, se a protecção de dados pessoais era até há pouco tempo tema desconhecido do grande público, num ápice passou a ser o *olho do furacão*, gerando leque preenchido de atropelos e violações de dados dos seus titulares. E a autoridade nacional de controlo continua amarrada a constrangimentos de índole múltipla, desde orçamentais à falta de recursos, humanos e tecnológicos. Imaginem o que escapa ao *mainstream* mediático.

Enquanto isso, a evolução do digital continua em passo acelerado. O nível de ameaça ao estado de direito democrático acompanha esta desenfreada marcha.

2 Disponível em https://www.dn.pt/lusa/interior/protecao-de-dados-condena-clinicas-que-recusam-tratar-doentes-por-falta-de-assinaturas-10901005.html,

Infelizmente, o tempo do direito e da justiça teimam em não se adaptar. Está assíncrono. O que, se por um lado até poderá induzir-nos a alguma prudência, por outro pode indiciar um factor de preocupação acrescido. Até pelo nível de risco em que coloca a sociedade, no seu todo.

Pensemos na utilização do uso de UAV's; na condução autónoma de veículos; na constante violação das propriedades essenciais da informação gerando supremacias informacionais ilegais a certos Estados; na massificação das redes sociais; na disseminação em *live streaming* de ataques a pessoas; na dispersão de conteúdo mentiroso e propagandístico *online* para desvirtuar o resultado de eleições livres e democráticas; na disseminação de ódio e violência *online*; nas novas ameaças a toda a actividade policial e de segurança do Estado; no controlo e rastreio individual *online* e no registo de crédito social em função disto; entre outras. A profusão destas notícias é de conhecimento geral. A *digitalização* humana está em curso. O ciberespaço, aparentemente, evolui para uma antiutopia.

Neste ensamble, vertiginoso e fulminante, é pois inconcebível que dois anos volvidos após um pedido de fiscalização sucessiva intentado junto do Tribunal constitucional português, por parte de um conjunto de partidos políticos, este Tribunal ainda não se tenha pronunciado quanto à constitucionalidade do acesso aos metadados, dados de tráfego e duração de comunicações por parte dos serviços secretos portugueses. É inconcebível e preocupante pois que, por um lado o serviço de informações da república esteja parado ou a trabalhar à margem da lei ante esta omissão do Tribunal; por outro lado, é inconcebível que este Tribunal, por excelência, de garantia dos direitos e liberdades fundamentais das pessoas, esteja dois anos para aferir da constitucionalidade de uma dada lei.

O que tanto demora a tomada de decisão? Falta de preparação temática dos juízes do Constitucional? Má técnica legislativa? Teimosia política? Falta de ameaças concretas, conhecidas do público, à segurança do Estado? Neste particular dos metadados, sublinho, o delírio é a nota dominante. Até porque, se *o Sistema de Acesso ao Pedido de Dados aos Prestadores dos Serviços de Comunicações Electrónicas (Sapdoc), foi declarado operacional pelo CFSIRP desde Março e está a funcionar*, no outro plano da acção, consta que poderá estar na iminência *um novo chumbo dos juízes,*

uma vez que a questão de fundo - violação do artigo 34º da CRP- manter-se-á [3]. Ora, parece-nos que este delírio, portanto, promete e vai continuar. Novo procedimento, novas discussões, nova lei, mais discussões, novo pedido de fiscalização, novo entorpecimento, novo regresso ao ponto de partida, que recordo, é a nota dominante desde que o poder político criou o *novo regime do Sistema de Informação da República Portuguesa*, em 2015.

Óbice daqui, ameaça dali, risco dacolá, não haverá uma luz de esperança que contrarie o delinear desta *antiutopia*?

A bem de todos nós, mesmo que tenha passado despercebido o *Christchurch Call*[4], julgamos decisivo o apelo à acção. Até porque o momento, o tempo e o espaço a tal nos obrigam. Aqui chegados, impõe-se-nos o sublinhar de parte das notas dos proponentes iniciais. Por um lado, o *envisage* do Presidente francês, o sr. Macron: «"*We need to build this new cyberspace, a free, open and secure Internet, which allows everyone to share, learn, innovate, but which also allows us to uphold our values, protect our citizen and empower them*"»; por outro, o apelo à adesão pluriparticipada, mundial, a cargo da Primeiro-Ministra Neozelandesa, a sra. Ardern: «"*From here, I will work alongside others signed up to the Christchurch Call to bring more partners on board, and develop a range of practical initiatives to ensure the pledge we have made today is delivered*"». Por um *mundo*, terreno e digital, melhor, de todos e para todos.

Por fim, num plano nacional, com especial saudação para a ousadia da proposta, arbitramos da pertinência do Projeto de Lei 1217/XIII[5], apresentado pelo partido Socialista, já apelidado de Carta de Direitos Fundamentais na Era Digital.

A Carta deverá corresponder a *lei de protecção de direitos, liberdades e garantias centrada nas pessoas, consagradora de valores democráticos essenciais contra ameaças que não devem ser ignoradas* procurando ir além de mera *lei compilatória das normas que na ordem jurídica portuguesa consagram (alguns) direitos*, que enuncie *um elenco diversificado e abrangente, que inove, clarifique e valha também*

3 https://www.dn.pt/poder/interior/-necessidade-inquestionavel-fiscais-das-secretas-validam-acesso-a-dados-das-comunicacoes--10935824.html

4 https://www.beehive.govt.nz/release/christchurch-call-eliminate-terrorist-and-violent-extremist-online-content-adopted

5 Disponível em: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768

como programa de ação vinculativo dos órgãos de poder, pode ler-se no enunciado programático do Projeto de lei. Deixo aqui um apelo a uma participação contributiva entusiasta por forma a melhorar este esboço inicial de consagração de uma Carta de Direitos Fundamentais na Era Digital.

Resta-me, a final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 24 de Maio de 2019

Nuno Teixeira Castro

CYBERLAW

by CIJIC

DOUTRINA

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

BRUNO PEREIRA [1]

E

JOÃO ORVALHO [2]

1 Instituto Politécnico de Beja
2 Instituto Politécnico de Beja

RESUMO

Uma Avaliação de Impacto sobre a Protecção de Dados (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.

Palavras-Chave: Dados pessoais; tratamento de dados pessoais; AIPD; Regulamento Geral de protecção de dados.

1. INTRODUÇÃO

Como é sabido, o RGPD - Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dado) veio revogar a Diretiva 95/46/CE, 24 de outubro de 1995, assim como Lei n.º 67/98, de 26 de outubro, a Lei da Proteção de Dados Pessoais, nas matérias com ele conflituantes (Monteiro, 2017).

Uma das principais inovações do RGPD consiste na previsão da obrigatoriedade de realização de avaliações de impacto sobre a proteção de dados (AIPD), ou em inglês *Data Protection Impact Assessment* (DPIA), quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares (artigo n.º 35, n.º 1 do RGPD) (Ramalho & Costa, 2017).

Esta técnica de avaliação de riscos no procedimento de tratamento de dados pessoais não é, em absoluto, inovadora, pois é bastante conceituada e utilizada nos países anglo-saxónicos, no entanto a sua regulamentação expressa no plano Europeu configura-se como uma das principais novidades do RGPD (Pica, 2018).

Em síntese, 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.

Assim, estas avaliações de impacto são instrumentos importantes em matéria de responsabilização, uma vez que ajudam os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequa- das para assegurar a conformidade com o regulamento (dando resposta ao artigo n.º 24 do RGPD). Por outras palavras, uma AIPD é um processo que visa estabelecer e demonstrar conformidade (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

As avaliações de impacto são da responsabilidade das próprias empresas ou organismos estatais que gerem os dados pessoais de clientes, fornecedores, parceiros ou trabalhadores.

Logo, nestas avaliações de impacto, deverão ser descritas as finalidades da recolha e tratamento de dados, os riscos inerentes à perda de informação, e a eventuais danos para as liberdades e garantias dos cidadãos (JusNet, 2018).

2. DOCUMENTO DE AVALIAÇÃO DE IMPACTO SOBRE PROTEÇÃO DE DADOS

Se Segundo o Grupo de Trabalho do Artigo 29.º (G29) [1] as AIPDs são definidas como: "*Um processo destinado a descrever o tratamento, avaliar a necessidade e proporcionalidade do tratamento e ajudar a gerir os riscos para os direitos e liberdades das pessoas singulares resultantes do tratamento de dados pessoais (avaliando-os e determinando as medidas para lidar com os mesmos)*" (Ramalho & Costa, 2017).

Embora, o RGPD não apresente uma definição direta de "risco", o Considerando 75 liga o conceito de risco ao dano potencial aos indivíduos, permitindo ao responsável pelos dados construir uma referência que o irá guiar pelo processo de avaliação do impacto.

De qualquer modo, o RGPD não exige a realização de uma avaliação de impacto para todas as operações de tratamento de dados. A realização de uma AIPD é obrigatória somente quando o tratamento for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo n.º 35, n.º 1 do RGPD), incluindo explicitamente alguma das três situações: "*avaliação sistémica e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado*" que sirva como base para "*decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar*", "*operações de tratamento em grande escala de categorias especiais de dados*" que são mencionados nos artigos n.º 9, n.º 1 e n.º 10, e "*controlo sistemático de zonas acessíveis ao público em grande escala*" (artigo n.º 35, n.º 3).

Para além dos três tipos de situações referidas no n.º 3 do artigo 35.º do RGPD, exige-se que as autoridades de controlo no território respetivo elaborem, tornem público e comuniquem uma lista das operações de tratamento sujeitas ao requisito de AIPD ao Comité Europeu para a Proteção de Dados (CEPD) (n.º 4 do artigo 35.º e alínea k do n.º 1 do artigo 57.º do RGPD) (CNPD, 2018; Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). É possível encontrar a lista da Comissão Nacional de Proteção de Dados (CNPD) de tratamentos de dados pessoais sujeitos a avaliações de impacto em (Diário da República, 2018).

Tal como referido (CNPD, 2018), a lista não é exaustiva, podendo ainda surgir, designadamente em função do desenvolvimento tecnológico, outras situações em que se justifique, nos termos do n.º 1 do artigo 35.º, realizar obrigatoriamente a AIPD. Por isso,

esta é uma lista dinâmica, sendo atualizada sempre que se entender necessário (CNPD, 2018). Esta lista também preenche os pressupostos do n.º 1 do artigo 35.º, e tem por referência os critérios presentes (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017) nas páginas 10 a 12 (CNPD, 2018).

Entre os critérios a ter em consideração para aferir da necessidade de realização de uma avaliação de impacto, incluem-se o tratamento de dados destinados a (I) avaliação e classificação dos titulares, designadamente *profiling* (ex: uma empresa que define perfis comportamentais baseados na navegação dos utilizadores do seu *website*), (II) tomadas de decisão automatizadas com efeito jurídico ou análogo, (III) monitorização sistemática, (IV) tratamento de dados sensíveis, que incluem os dados relativos a comunicações, a localização, a saúde, bem como os dados financeiros e, em certos casos, dados tratados para fins puramente pessoais (como em matéria de serviços de armazenamento na nuvem de informação pessoal ou de *apps* com registo de informação diária do utilizador), (V) tratamento de dados em grande escala, (VI) tratamentos de dados resultantes de uma interconexão; (VII) tratamento de dados relativos a indivíduos especialmente vulneráveis; (VIII) utilização inovadora ou aplicação de soluções tecnológicas ou organizacionais, tal como a combinação do uso de impressões digitais com reconhecimento facial para controlo de acessos; (IX) transferência de dados para países terceiros, (X) ou quando o tratamento impede o titular dos dados de exercer um direito ou utilizar um serviço ou contrato (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017; Ramalho & Costa, 2017).

No entanto, deve-se salientar que o Considerando 91 do RGPD dispõe, expressamente, que o "tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto não deverá ser obrigatória.". No que toca à "grande escala", o G29 refere que "apesar de o considerando dar exemplos relativos aos extremos da escala (tratamento por um médico por oposição ao tratamento de dados de um país inteiro ou à escala da Europa), existe uma extensa zona cinzenta entre estes dois extremos" (Grupo do Artigo 29.º para a Proteção de Dados, 2017).

De acordo com o G29, a verificação de mais do que um dos critérios deverá funcionar como indício da necessidade de realização de uma AIPD, sem prejuízo de essa necessidade de se poder verificar quando apenas um seja verificado (Ramalho & Costa, 2017). Na verdade, é considerada uma boa prática a realização de uma avaliação de impacto nestas condições. Por outro lado, uma operação de tratamento pode corresponder aos casos mencionados e

continuar a ser considerada pelo responsável como uma operação que não é suscetível de implicar um elevado risco. Consequentemente, este deve justificar e documentar as razões que o levam a não realizar uma AIPD e mencionar os pontos de vista do encarregado da proteção de dados (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Sempre que não seja claro se a realização de uma AIPD é necessária, o G29 recomenda que, ainda assim, seja realizado o procedimento, uma vez que é um instrumento útil para ajudar os responsáveis pelo tratamento a cumprir a legislação relativa à proteção de dados (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

O G29 considera que uma avaliação de impacto não é obrigatória nos seguintes casos (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017):

- Quando o tratamento não for "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (artigo n.º 35, n.º 1);

- Quando a natureza, o âmbito, o contexto e as finalidades do tratamento forem muito semelhantes ao tratamento em relação ao qual tenha sido realizada uma AIPD;

- Quando as operações de tratamento tiverem sido previamente controladas por uma autoridade de controlo antes de maio de 2018 em condições específicas que não se tenham alterado. Em contrapartida, algumas alterações também podem fazer baixar os riscos. Neste caso, a revisão da análise do risco efetuada pode revelar que a realização de uma AIPD deixa de ser obrigatória;

- Quando uma operação de tratamento, nos termos do artigo n.º 6, n.º 1, alíneas

c) ou e), tiver um fundamento jurídico no direito da UE ou de um Estado-Membro, em que o direito regule a operação de tratamento específica e em que a AIPD já tenha sido realizada como parte da adoção desse fundamento jurídico (artigo n.º 35, n.º 10), salvo se o Estado-Membro considerar necessário proceder a essa avaliação antes das atividades de tratamento;

- Quando o tratamento estiver incluído na lista opcional (definida pela autoridade de controlo) de operações de tratamento para as quais não é obrigatória uma AIPD (artigo n.º 35, n.º 5).

É importante referir que o simples facto de as condições que conduzem à obrigação de realizar uma AIPD não terem sido satisfeitas não os dispensa do cumprimento das restantes obrigações previstas no RGPD ou em legislação especial (CNPD, 2018). Na prática, tal significa que os responsáveis pelo tratamento devem avaliar continuamente os riscos criados

pelas suas atividades de tratamento por forma a identificarem quando um certo tipo de tratamento é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

A AIPD deve ser realizada "antes de iniciar o tratamento" (artigo n.º 35, números 1 e 10, e Considerandos 90 e 93 do RGPD). O que ocorre em coerência com os princípios da proteção de dados desde a conceção e por defeito (artigo n.º 25 e considerando 78 do RGPD). Além de que, estas avaliações de impacto devem ser encaradas como instrumentos de apoio à tomada de decisão em relação ao tratamento (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Tal como referido em (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017), uma avaliação de impacto deve ser iniciada o mais cedo possível na conceção da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas, sendo que deve existir uma atualização da mesma (AIPD) ao longo do ciclo de vida do projeto de modo a garantir que a proteção dos dados e a privacidade sejam consideradas e que seja incentivada a criação de soluções que promovem a conformidade. O facto de a AIPD poder necessitar de ser atualizada após o tratamento ter efetivamente sido iniciado não é uma razão válida para adiar ou não realizar a avaliação de impacto, visto que a mesma é um processo contínuo, especialmente quando uma operação de tratamento é dinâmica e está sujeita a mudanças permanentes.

Feita esta análise é possível, previamente, determinar as medidas que devem ser implementadas a fim de eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes (Pica, 2018).

Com base no artigo n.º 36, n.º 1, no caso da avaliação de impacto resultar que as operações a realizar colocam em risco a esfera jurídica do titular destes dados pessoais, e na ausência de medidas que afastam ou atenuem o risco (através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação (Magalhães & Pereira, 2018), deve o responsável pelo tratamento consultar, previamente às operações de tratamento, a entidade de controlo (a CNPD em Portugal) devendo comunicar-lhe quem é o responsável pelo tratamento, as finalidades e os meios de tratamento previstos, as medidas e garantias previstas para salvaguardar os direitos e liberdades dos titulares dos dados pessoais, os contactos do encarregado dos dados pessoais (caso este exista na entidade responsável), o resultado da avaliação de impacto e, ainda, todas as informações que a entidade de controlo venha a solicitar (Pica, 2018).

De acordo com o G29, estão em causa casos em que os riscos identificados não podem ser suficientemente endereçados pelo responsável pelo tratamento (ex: quando os riscos residuais se mantêm elevados), como, a título de exemplo, situações em que os titulares dos dados se podem deparar com consequências significativas (ou até irreversíveis) que não podem ultrapassar, e/ou quando aparenta ser óbvio que o risco ocorrerá (Coutinho & Moniz, 2018).

Caso a autoridade de controlo considerar que o tratamento viola o previsto no RGDP, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deverá, no prazo de oito semanas a contar da receção do pedido de consulta, emitir orientações a este responsável ou, quando aplicável, ao subcontratante, podendo recorrer a todos os seus poderes referidos no artigo 58.º (artigo 36.º, n.º 2) (Coutinho & Moniz, 2018).

Na Figura 1 (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017) é possível verificar uma ilustração dos princípios básicos relacionados com a AIPD no RGPD.

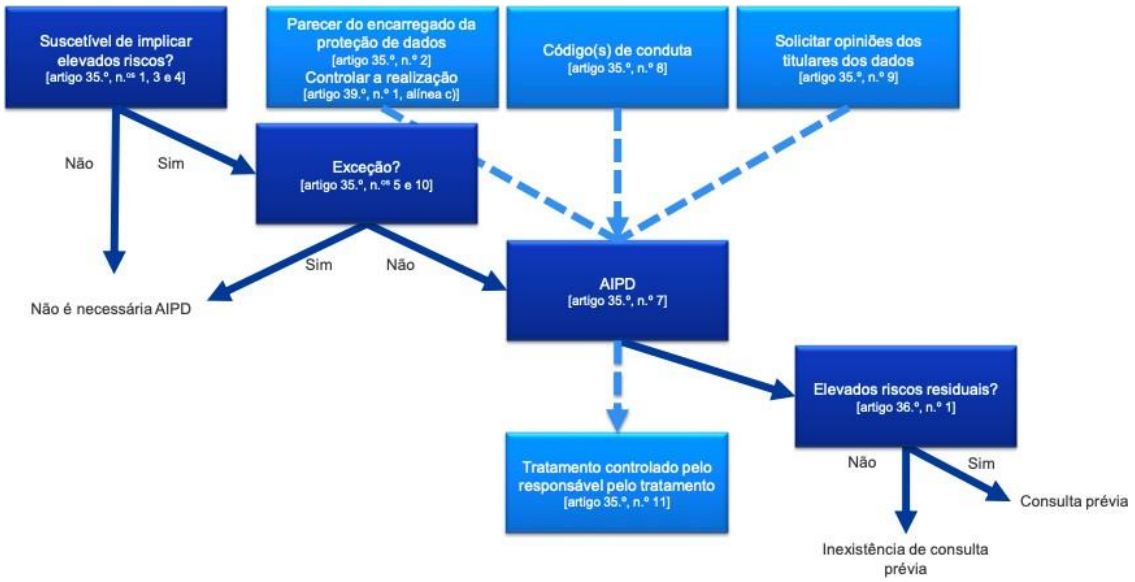

Figura 1. Princípios básicos relacionados com a AIPD no RGPD

Antes de mais, é preciso acentuar que o responsável pelo tratamento está incumbido de garantir a realização da AIPD (artigo n.º 35, n.º 2). Ainda que a realização da avaliação de impacto possa ser efetuada por outrem, dentro ou fora da organização, este responsável continua a ser o responsável último por essa tarefa (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). Este responsável deve também solicitar o parecer do

encarregado da proteção de dados, nos casos em que este tenha sido designado (artigo n.º 35, n.º 2), sendo que o seu parecer e as decisões tomadas pelo responsável pelo tratamento devem ser documentadas na AIPD (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

No caso de o tratamento for total ou parcialmente efetuado por um subcontratante, o subcontratante deve auxiliar o responsável pelo tratamento na realização da AIPD e fornecer todas as informações necessárias (em consonância com o artigo n.º 28, n.º 3, alínea f) (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Nos termos do RGPD, a não conformidade com os requisitos de uma AIPD pode conduzir à imposição de coimas pela autoridade de controlo competente. Não realizar uma AIPD quando o tratamento está sujeito a uma avaliação de impacto (artigo 35.º, n.º 1 e números 3 a 4), realizar uma AIPD de forma incorreta (artigo 35.º, n.º 2 e n.ºs 7 a 9) ou não consultar a autoridade de controlo competente quando necessário (artigo 36.º, n.º 3, alínea e), pode resultar numa coima administrativa de até 10 milhões de euros ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

3.ABRANGÊNCIA DE AIPD

Por outro lado uma única avaliação de impacto pode ser utilizada para avaliar múltiplas operações de tratamento que sejam semelhantes em termos de natureza, âmbito, contexto, finalidade e riscos. A título de exemplo, se as autoridades ou organismos públicos pretendessem criar uma aplicação de tratamento comum, esta poderia ser abrangida apenas com uma AIPD (Pinheiro, Gonçalves, Gonçalves, Coelho, & Duarte, 2018).

Na verdade, as avaliações de impacto visam estudar sistematicamente novas situações que possam ser suscetíveis de implicar riscos elevados para os direitos e as liberdades das pessoas singulares, não havendo necessidade de realizar uma AIPD para os casos que já foram estudados (ou seja, operações de tratamento realizadas num contexto específico e com uma finalidade específica). Pode também ser aplicável a operações de tratamento semelhantes aplicadas por vários responsáveis pelo tratamento de dados. Nestes casos, deve ser partilhada ou disponibilizada ao público uma AIPD de referência, devem ser adotadas as medidas descritas na avaliação de impacto e deve ser fornecida uma justificação para a realização de uma única avaliação de impacto (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Quando a operação de tratamento envolve responsáveis conjuntos pelo tratamento, estes devem definir detalhadamente as respetivas obrigações. A AIPD deve definir qual das partes é responsável pelas várias medidas concebidas para dar resposta aos riscos e proteger os direitos e as liberdades dos titulares dos dados. Cada responsável pelo tratamento de dados deve exprimir as suas necessidades e partilhar informações úteis sem comprometer segredos (ex: proteção de segredos comerciais, propriedade intelectual, informações empresariais confidenciais) ou revelar vulnerabilidades (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

4. METODOLOGIA PARA REALIZAÇÃO DE UMA AIPD

Existem metodologias diferentes, todavia os critérios (presentes no anexo 2 de (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017)) são comuns. O RGPD define os elementos mínimos de uma avaliação de impacto (artigo n.º 35, n.º 7, e considerandos 84 e 90), sendo eles:

- Uma descrição das operações de tratamento previstas e a finalidade do tratamento;
- Uma avaliação da necessidade e proporcionalidade das operações de tratamento;
- Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

E as medidas previstas para:

- fazer face aos riscos;
- demonstrar a conformidade com o Regulamento.

Recordemos que uma 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. Em contrapartida, a gestão dos ris- cos noutros domínios (ex: segurança da informação) centra-se na organização (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Numa perspetiva organizacional, a execução de uma AIPD serve não só para estar em harmonia com a lei, evitando coimas avultadas, mas também para melhorar a reputação da empresa aos olhos dos indivíduos cujos dados são processados, demonstrando um maior nível de transparência do que se verificava no passado. Podem também surgir benefícios financeiros, tendo em conta que identificar um problema cedo significa, de forma geral, que a sua solução será menos cara do que se o mesmo problema fosse descoberto mais tarde.

As avaliações de impacto servem, assim, como uma parte vital da proteção por *design*, pois visam garantir que se está em conformidade perante a proteção de dados desde o início de um projeto.

Procurando facilitar a tarefa dos responsáveis, o G29 disponibilizou um anexo com os critérios mínimos para uma AIPD aceitável, tendo como base quatro pilares: um descrição sistemática das operações de tratamento dos dados, uma avaliação da necessidade e proporcionalidade dos tratamentos para os efeitos desejados, a garantia de que os riscos para

os direitos e liberdades dos titulares dos dados são geridos e que as partes interessadas (encarregado da proteção de dados, titulares dos dados) são envolvidas no processo (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

No entanto, e tendo em conta que não existe nenhum modelo totalmente padronizado para realização de uma avaliação de impacto, é possível, e até desejável em algumas ocasiões, a utilização de um *template* existente do que a criação de um novo documento de raiz, apenas baseado nos critérios.

Por sua vez e por exemplo, no Reino Unido, um órgão independente, a *Information Commissioner's Office* (ICO), disponibiliza um modelo de realização de uma AIPD (Information Comissioner's Office, 2018b), composto por sete passos, muito completo, e que deverá ser suficiente para uma primeira abordagem às AIPDs. A tabela 1 representa e explica os conteúdos dos passos do modelo.

Tabela 1

Passos do Modelo AIPD da ICO

Passos	**Pontos Importantes**
1. Identificação da necessidade para realização de uma AIPD	Em que consiste o projeto: - objetivo; - tipo de tratamento. Usado em conjunto com a lista de casos em que uma AIPD deve ser realizada, fundamentando cada ponto.

2. Descrição do tratamento	Natureza do tratamento: - como se vão coletar, usar, armazenar e eliminar dados; - qual é a fonte dos dados; - partilha de dados. *Scope* do tratamento: - natureza dos dados (inclui categorias especiais ou registos criminais?); - quantidade de dados coletados e usados; - frequência do tratamento; - duração do armazenamento; - número de titulares possivelmente afetados; - área geográfica que o tratamento cobre. Contexto do tratamento: - natureza da relação com os titulares; - quantidade de controlo por parte dos titulares; - expectativas dos titulares em relação ao tratamento; - inclusão de grupos vulneráveis; - preocupações relativamente ao tipo de tratamento ou possíveis falhas de segurança - utilização de novas tecnologias; - existência de questões de interesse

	público; - códigos de conduta ou certificações estabelecidas. <u>Propósito do tratamento:</u> - interesses legítimos; - resultado pretendido para os titulares; - benefícios esperados para a organização ou sociedade em geral.

3. Consulta	Consulta dos titulares: - quando e como se vão procurar e documentar as opiniões dos titulares. Consulta de outros: - consulta de intervenientes internos; - consulta de pessoal externo, caso necessário - peritos em lei, IT, etc.
4. Avaliação da necessidade e proporcionalidade	Descrição de medidas de conformidade e proporcionalidade: - base legal para o tratamento; - cumprimento do objetivo estabelecido; - possíveis formas alternativas de cumprir o objetivo; - prevenção contra *function creep*; - medidas para garantir a qualidade dos dados; - medidas para limitar o uso dos dados; - como se informam os titulares relativamente à privacidade; - como se implementam os direitos dos titulares; - salvaguardas relativamente a transferências internacionais.

5. Identificação e avaliação de riscos	<u>Descrição da fonte dos riscos e possíveis impactos nos titulares, em particular no que possa contribuir para:</u> - inabilidade de exercer direitos; - inabilidade de aceder a serviços ou oportunidades; - perda de controlo sobre o uso dos dados pessoais; - discriminação; - roubo de identidade ou fraude; - perdas financeiras; - danos reputacionais; - dano físico; - perda de confidencialidade; - qualquer outra desvantagem económica ou social. Construir uma matriz que cruze a gravidade do impacto com a probabilidade de ocorrência.
6. Identificação de medidas de mitigação	Medidas para reduzir ou eliminar os riscos identificados no passo n.º 5.

7. Assinaturas e resultados	Registar: - medidas adicionais a tomar; - se cada risco foi eliminado, reduzido ou aceite; - o nível geral de risco após implementação das medidas; - necessidade de consultar a CNPD; - aconselhamento do encarregado da proteção de dados.

Este modelo, em conjunto com os recursos disponibilizados pela CNPD, coloca os parâmetros para realizar uma avaliação de impacto competente.

Num esforço para simplificar a compreensão do que consiste uma AIPD, Pinheiro *et al.* dividem o processo em três fases: descritiva, onde se descrevem as operações de tratamento, a finalidade e os interesses legítimos do responsável; avaliativa, com base no princípio da proporcionalidade, em que se avaliam a relação entre as operações e os objetivos, bem como os riscos para os direitos e liberdades dos titulares; decisória, centrando-se nas medidas previstas para fazer face aos riscos (Pinheiro et al., 2018).

Já Saldanha (Saldanha, 2018) divide o procedimento em quatro partes: iniciação do projeto, onde se define o objetivo da AIPD, antes do começo do tratamento; análise do fluxo de dados, levando-se a cabo o mapeamento de informações pessoais, "criando um fluxograma de como a informação pessoal atravessa a organização, como resultado das atividades"; análise de privacidade, com recurso a questionários; relatório de avaliação de impacto de privacidade, onde se apresentam a avaliação dos riscos de privacidade, para além da implicação desses riscos e formas de mitigação, se possível.

Existem também soluções de *software* pagas cujo objetivo é facilitar o processo de realização de avaliações de impacto, como os produtos da *OneTrust* (OneTrust, 2018) e *Vigilant Software* (Vigilant Software, 2018), com recurso a ferramentas automatizadas que são integradas nos ciclos de vida dos projetos.

É importante também referir que a ISO/IEC 29134:2017 fornece uma diretriz detalhada sobre como executar uma AIPD e como manter evidências disso (Ruehl & Harvey, 2018).

5. DISCUSSÃO

Como já abordado, a AIPD é uma forma útil de garantir que existe conformidade perante a lei desde o início de um projeto. É possível, desta forma, evitar coimas avultadas que poderiam terminar pequenas e médias empresas sem capacidade financeira suficiente para as suportar. No entanto, na nossa opinião, são de facto estas empresas que estão em maior risco de cometer infrações, ainda que sem intenção.

Com esta análise de impacto consegue-se desde logo identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem (Pica, 2018). É ainda importante considerar que o risco pode resultar não só da ineficiência das medidas de segurança adotadas, mas também de espetos inerentes à própria natureza dos dados do tratamento em questão (Coutinho & Moniz, 2018).

Isto sem esquecer que os responsáveis pelo tratamento de dados devem ter em conta um conjunto de considerações éticas no momento de conceção do próprio processo de tratamento, devendo interromper o mesmo, caso os risco aos direitos e liberdades do indivíduos inerentes ao processo sejam elevados (Coutinho & Moniz, 2018).

No que se refere à frequência da realização de avaliações de impacto, é recomendado que seja um processo contínuo, integrado na metodologia de desenvolvimento adotada pela empresa, o que leva à questão: o que acontece quando uma pequena empresa não segue nenhuma metodologia específica?

A ausência de um bom planeamento ou estrutura numa empresa pode levar a que as AIPDs não sejam realizadas periodicamente, o que significa que podem surgir casos onde é feito o tratamento de dados pessoais entre AIPDs, sem que tal seja explícito nas mesmas. Nestas situações, as organizações correm o risco de não estar em concordância com o RGPD. Por esta perspetiva, as avaliações de impacto servem como motivação para até as pequenas empresas terem uma estrutura sólida que lhes permita desenvolver os seus projetos de forma organizada, demonstrando conformidade pelo caminho, construindo uma base para a evolução da empresa.

Além disso, os limitados recursos financeiros das pequenas empresas também impõem um obstáculo no que toca à consulta de peritos que possam garantir uma AIPD bem feita. Neste procedimento há muitos pontos que podem falhar, tendo em conta a lista de condições que compõem uma AIPD competente. Em pequenas empresas, especialmente naquelas onde não

existe um encarregado da proteção de dados, recai sobre o responsável pelo tratamento a grande maioria da realização da avaliação de impacto, levando a que possa escapar algo que vá contra o RGPD. Sem recurso a peritos externos nem a *software* pago, esta situação poderá acontecer facilmente.

Algo que poderia ajudar qualquer tipo de empresa/organização a realizar boas AIPDs seria a publicação de relatórios por parte de desenvolvedores de *software*, onde seriam enumerados todos os pontos cujo *software* poderá infringir sem as devidas precauções. Deste modo, os responsáveis sobre tratamento de dados teriam acesso a uma lista mais restrita de critérios a ter em conta, tendo em vista os *softwares* usados no projeto.

Resumindo, existem diversos desafios aquando da realização de uma AIPD, nomeadamente: o medo de ao realizar uma AIPD estar a restringir as opções e práticas de negócio, a falta de informação para permitir uma AIPD ser criada completamente, a conotação negativa da AIPD por estar associada a um trabalho árduo e que requer bastante tempo, a resistência à mudança (por parte das pessoas) que frequentemente está presente, entre outros desafios (Shad, 2018).

Os obstáculos impostos pela obrigatoriedade da realização de avaliações de impacto podem levar a que os responsáveis pelo tratamento de dados as interpretem como custos adicionais e tarefas desnecessárias, e não apenas como algo útil tanto para a organização, como também para os titulares dos dados.

6. CONCLUSÕES

Uma AIPD, tal como a maioria dos exercícios de avaliação de risco, encoraja a verificar cuidadosamente: o que se está a fazer, porque se está a fazer, os riscos envolvidos e como se está a controlar esses riscos a um nível aceitável (Macaskill, 2018; Messenger-Clark, 2017).

As avaliações de impacto são uma forma útil de os responsáveis pelo tratamento de dados aplicarem sistemas de tratamento de dados que estejam em conformidade com o RGPD, podendo ser obrigatórias para alguns tipos de operações de tratamento. Os responsáveis pelo tratamento de dados devem encarar a realização de uma AIPD como uma atividade útil e positiva que ajuda à conformidade jurídica (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

Visto que a realização da AIPD implica a avaliação do impacto das operações de tratamento, tem também a vantagem de promover implicitamente o cumprimento do Código de Conduta estabelecido no artigo 40.º do RGPD. Com esta análise de impacto é possível identificar os possíveis riscos para a proteção dos dados pessoais dos afetados e a valorização da probabilidade de ocorrerem, bem como os danos que causariam se se materializassem. Feita análise é possível, previamente, determinar as medidas que devem ser implementadas com vista a eliminar ou mitigar os riscos detetados, permitindo adotá-los no tratamento dos dados pessoais a fim de concretizar a tutela dos direitos fundamentais dos titulares destes (Pica, 2018).

A realização de uma avaliação de impacto é um processo contínuo e não um exer- cício que acontece uma única vez. Por uma questão de boa prática, uma AIPD deve ser continuamente revista e regularmente reavaliada (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017). Como o tratamento de dados é uma realidade mutável, é recomendável que as AIPDs sejam continuamente realizadas para tratamentos de dados em curso, devendo ser reavaliadas no prazo máximo de três anos, sem prejuízo de prazo inferior se impor em função das circunstâncias do caso (Ramalho & Costa, 2017).

Algumas empresas identificam corretamente situações onde é necessário a realização de uma AIPD, todavia apenas a fazem quando um projeto já muito progrediu, levando a que seja menos provável de ajudar a respeitar totalmente os requisitos do RGPD aquando da realização da avaliação de impacto. Além disso, os custos podem aumentar, no caso de um sistema necessitar de ser re-especificado ou corrigido (Clarke, 2018).

O RGPD dá aos responsáveis pelo tratamento de dados a flexibilidade necessária para determinar a estrutura e a forma precisas da AIPD com vista a que esta se encaixe nas práticas de trabalho existentes (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

As avaliações de impacto tratam-se de um mecanismo de gestão de risco dos direitos dos titulares dos dados e não da organização, devendo ser adaptada à realidade de cada organização (Ramalho & Costa, 2017). A publicação de uma avaliação de impacto não é um requisito jurídico do RGPD, essa decisão recai sobre o responsável pelo tratamento. Contudo, os responsáveis pelo tratamento devem considerar, pelo menos, a publicação parcial da AIPD, por exemplo, um resumo ou uma conclusão. Porém, esta publicação parcial ajuda a fomentar a confiança nas operações de tratamento de dados do responsável e a demonstrar responsabilidade e transparência (Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, 2017).

REFERÊNCIAS BIBLIOGRÁFICAS

Clarke, O. (2018). *Data Protection Impact Assessments under GDPR - Osborne Clarke | Osborne Clarke.* Consultado em 2019-01-22. Disponível: http://www.osborneclarke.com/insights/data-protection-impact-assessments-under-gdpr/CNPD. (2018). *Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a avaliação de impacto sobre a proteção de dados* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/decisoes/regulamentos/regulamento_1_2018.pdf

Coutinho, F., & Moniz, G. (2018). *Anuário de Protecção de Dados*. CEDIS.

Diário da República. (2018). *Regulamento 798/2018, 2018-11-30 - DRE*. Consultado em 2018-12-17. Disponível: https://dre.pt/web/guest/pesquisa//search/117182365/details/normal?l=1

European Data Protection Board. (2018). *Grupo de Trabalho do Artigo 29.º*. Consultado em 2019-01-24. Disponível: https://edpb.europa.eu/our-work-tools/article-29-working-party

Grupo de Trabalho do Artigo 29.º para a Proteção de Dados. (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* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf

Grupo do Artigo 29.º para a Proteção de Dados. (2017). *Orientações sobre os encarregados da proteção de dados (EPD)* (Tech. Rep.). Disponível: https://www.cnpd.pt/bin/rgpd/docs/wp243rev01_pt.pdf

Information Comissioner's Office. (2018a). Data Protection Impact Assessments (DPIAs). Disponível: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

Information Comissioner's Office. (2018b). *Sample DPIA template* (Tech. Rep.). Disponível: https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

JusNet. (2018). *Jusjornal - Documento.* Consultado em 2018-12-17. Disponível: http://jusnet.wolterskluwer.pt/Content/DocumentMag.aspx?params=H4sIAAAAAAAEAMtMSbH1czUAASMDQxNLtbLUouLM_DxbIM_CwNzQAiSQmVbpkp8cUlmQapuWmFOcqpaYVJyfU1qSGlqUaRtSVJoKADuZV9BGAAAAWKE

Macaskill, R. (2018). *So, What is a Data Protection Impact Assessment and Why Should Organizations Care? - DATAVERSITY.* Consultado em 2019-01-22. Disponível: https:// www.dataversity.net/data-privacy-impact-assessment-organizations-care/

Magalhães, F., & Pereira, M. (2018). *Regulamento Geral de Protecção de Dados* (2nd ed.). Porto: VidaEconómica.

Messenger-Clark, R. (2017). *Data Protection Impact Assessment* (Tech. Rep.). Disponível: http:// www.leeds.ac.uk/secretariat/documents/dpia.pdf

Monteiro, P. (2017). *Está preparado para o novo Regulamento Geral sobre a Protecção de Dados?| Human Resources.* Consultado em 2018-12-13. Disponível: https://hrportugal.pt/esta-preparado-para-o-novo-regulamento-geral-sobre-a-proteccao-de-dados/

OneTrust. (2018). *PIA & DPIA Automation | Products | OneTrust.* Consultado em 2019-01-03. Disponível: https://www.onetrust.com/products/assessment-automation/

Pica, L. (2018). *As avaliações de impacto, o encarregado de dados pessoais e a certificação no novo regulamento europeu de proteção de dados pessoais*. CYBERLAW by CIJIC. Disponível: 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

Pinheiro, A., Gonçalves, C., Gonçalves, C., Coelho, C., & Duarte, T. (2018). *Comentário ao Regulamento Geral de Proteção de Dados* (12-2018 ed.). Edições Almedina.

Ramalho, D., & Costa, T. (2017). *LEGAL ALERT* (Tech. Rep.). Disponível: https://www.mlgts.pt/xms/files/v1/Publicacoes/Newsletters_Boletins/2017/Legal_Alert_-_Nova_orientacao_do_grupo_de_trabalho_do_artgio_29.pdf

Ruehl, U., & Harvey, J. (2018). *Data Protection Management Systems and the GDPR - General Data Protection Regulation (GDPR) | TUV USA*.Consultado em 2019-01-22. Disponível: https://www.tuv-ord.com/us/en/technology-it/general-data-protection-regulation-gdpr/data-protection-management-systems-and-the-gdpr/

Saldanha, N. (2018). *Novo Regulamento Geral de Proteção de Dados* (1st ed.). FCA - Editora de Informática.

Shad, A. (2018). *Do I need a Data Protection Impact Assessment to avoid GDPR fines? | ECOM- PLY.io*. Consultado em 2019-01-22. Disponível: https://ecomply.io/do-i-need-a-data-protection-impact-assessment-to-avoid-gdpr-fines/

Vigilant Software. (2018). *Data Protection Impact Assessment Tool | Vigilant Software*. Consultado em 2019-01-03. Disponível: https://www.vigilantsoftware.co.uk/topic/dpia