# Indice

[**QUESTAO 1**](#_bb0v3cxuxify) **4**

[Justifique e fundamente a conciliação jurídica possível, em caso de colisão, entre os direitos “ao bom nome e reputação” e “à palavra e à imagem” consagrados no n.º 1 do artigo 26º da CRP, e os direitos de “informar, de se informar e de ser informados, sem impedimentos nem discriminações” consagrados no n.º 1 do artigo 37º da CRP.](#_ahpsqnvpyguh) 4

[Resposta](#_cxijxz56w6ab) 4

[**QUESTAO 2**](#_prhjufoplex4) **5**

[No âmbito da Lei do Cibercrime, tipifique os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos, facultando um exemplo de cada uma das tipificações. Fundamente a resposta com a própria lei.](#_q21r7jbt8xxo) 5

[Resposta](#_olz2j881ungm) 5

[**QUESTAO 3**](#_frq0mrnwsrdt) **7**

[O Governo português elaborou um projeto de lei que pretende obrigar as instituições públicas e as instituições privadas de solidariedade social (IPSS) a divulgarem o nome dos beneficiários de apoios sociais, de qualquer natureza, através da página de internet da Inspeção Geral de Finanças. Exponha, no seu entendimento, quais os limites legais que esta medida pode enfrentar, e que meios jurídicos tem o Governo para salvaguardar a legalidade constitucional do referido diploma.](#_9tmvre5kixe) 7

[Resposta](#_wbciejz8cvjy) 7

[**QUESTAO 4**](#_ckq48mxjz8il) **9**

[O RGPD visa garantir os direitos dos titulares dos dados pessoais. Descreva quais são os direitos dos titulares de dados, providenciando exemplos de como podem ser colocados em prática. Fundamente a resposta.](#_7myxcni2738z) 9

[Resposta](#_o9zkwlgg0pg5) 9

[**QUESTAO 5**](#_pa4a8892cr6) **11**

[Fundamente o princípio jurídico da proteção constitucional dos direitos consagrados no artigo 34º da CRP sobre a correspondência e o sigilo das telecomunicações, e as obrigações do Estado de garantir aos cidadãos um combate eficaz contra o crime organizado e contra o terrorismo. Justifique a resposta ligando estas temáticas ao RGPD.](#_x1iyz6xo3vdc) 11

[Resposta](#_d4r4lbz1r2mu) 11

[**QUESTAO 6**](#_s3ekmlbzvknx) **15**

[O RGPD estabelece regras relativamente ao tratamento dos dados pessoais dos candidatos a ofertas de emprego. Elabore um método completo para a obtenção da legitimidade para o tratamento de dados em candidaturas de emprego. Fundamente a resposta.](#_zdddplnlwis9) 15

[Resposta](#_u2slfwkgjq47) 15

[**QUESTAO 7**](#_xurp7vxb2z93) **16**

[Quais as obrigações a que está sujeita qualquer empresa ou organização em matéria de proteção de dados pessoais, e que funções estão reservadas à Comissão Nacional de Proteção de Dados. Fundamente a resposta.](#_o74h9dkws1tj) 16

[Resposta](#_pxzzaeq4taer) 16

[**QUESTAO 8**](#_lt1d9qhvhs75) **17**

[O comércio eletrónico é cada vez mais utilizado nas economias modernas. Exponha quatro direitos que os consumidores têm para exigirem o integral cumprimento dos contratos que podem celebrar com suporte em plataformas eletrónicas, nomeadamente no que respeita às garantias de equipamentos ou sobre a qualidade dos produtos encomendados a fornecedores com sede em países da União Europeia. Justifique a resposta, com base na Lei do Comércio Eletrónico.](#_imtwpmonusmy) 17

[Resposta](#_mgzpqyngpgor) 17

[**QUESTAO 9**](#_zdmfxl8ty6bo) **18**

[Os colaboradores das empresas são também titulares de dados pessoais. Descreva em detalhe que ações deverá efetuar o empregador para que se cumpra o RGPD relativamente a estes dados. Fundamente a resposta.](#_icrfqw6dwgeh) 18

[Resposta](#_ru7ho11mdgao) 18

[**QUESTAO 10**](#_81iib63wlyo0) **19**

[Exponha dois instrumentos jurídicos a que pode recorrer um criador de software de jogos de diversão para salvaguardar os seus direitos de propriedade intelectual, quando presta serviços a uma empresa na condição de trabalhador dependente. Fundamente a resposta com dois exemplos práticos, e com os correspondentes instrumentos legais.](#_4vioxb25vyr) 19

[Resposta](#_szcxgmmmu96x) 19

[**QUESTAO 11**](#_svhflqarkejv) **21**

[Os direitos à liberdade de expressão e de informação não são absolutos, e têm de ser conciliados com outros direitos de igual relevância constitucional. Justifique como conciliar os direitos dos jornalistas à publicação de notícias de relevante interesse público, e os direitos à reserva da vida privada e familiar de figuras públicas que desempenham cargos políticos. Justifique a resposta com os normativos constitucionais aplicáveis.](#_xreoafh2edyt) 21

[Resposta](#_4y2hygqe8kq6) 21

[**Questao 12**](#_r40mfo16lkkx) **23**

[A concentração excessiva dos capitais das empresas de media e o cruzamento de capitais entre grupos com os mesmos sócios ou acionistas é proibida na Constituição da República Portuguesa. Faça o enquadramento jurídico dessa questão, quer ao nível da CRP, quer ao nível da Lei da Imprensa, relevando ainda as funções que cabem à ERC nesta mesma matéria. Fundamente a resposta identificando e transcrevendo os preceitos legais aplicáveis.](#_jw6sbwns3oz1) 23

[**Decreto de aprovação da Constituição**](#_jka7qepjg3s9) **24**

[**Decreto de aprovação da Constituição**](#_trsnwuiqhcmn) **24**

[**Questao 13**](#_3yc8qbivyjay) **25**

[O Estatuto do Jornalista, enquanto lei da República, estabelece deveres muito concretos aos profissionais do setor. Identifique esses mesmos deveres, fazendo um estudo comparativo entre eles e os mesmos preceitos consagrados no Código Deontológico o Jornalista. Fundamente a resposta com a transcrição dos referidos deveres nos dois instrumentos jurídicos.](#_oo9z2jpnh3h8) 25

[**Video TEDX Conclusao**](#_9bmwtthey0ix) **28**

[Comentário Nuno:](#_szhqxpb5dim0) 29

[**RGPD Perguntas da Aula**](#_2eyavyjewbj5) **30**

[**Explique por suas palavras o que e o RGPD**](#_yep0kuf496ur) **30**

[**Dos paises da uniao europeia qual e a idade que consideram uma “criança”**](#_ewewjgtunsoe) **30**

[**O que considera ser dados pessoais?**](#_umh3k2fpwp5s) **31**

[**A quem se aplica o RGPD?**](#_5w5mr3k8x6yn) **31**

[**Defina as categorias de dados pessoais abrangidos pelo RGPD**](#_2u6dl9hn1opd) **31**

[**Quais a exigências do RGPD**](#_91ya65o95g2i) **32**

[**Princípios gerais do RGPD**](#_bo6m7c2q2yjj) **32**

[**Escreva por suas palavras as possíveis medidas de licitude nas operações**](#_c4jlwdtpt6l7) **33**

[**Descreva por suas palavras o que é a accountability**](#_pyfjpjqd10vw) **34**

[**Qual e a diferenca entre o accountability, a prova e evidência do cumprimento e a licitude nas operações**](#_g2s61tat725p) **35**

[**Descreve por suas palavras os novos direitos, indicando como podem ser exercidos e que penalizações poderao existir para quem nao os comprir**](#_1icwjwjp2ruk) **35**

[**Descreva por suas palavras quais as entidades ao qual não se aplicam as medidas de direitos, adaptação e prova do RGPD?**](#_pzqv3iq9nz14) **37**

[**Privacy by design & Privacy by default**](#_foc61m4ry9w2) **37**

[**As responsabilidades dos responsáveis pelo tratamento ou subcontratados não estabelecidos na união europeia(ex: como os dados da google saem cá para fora)?**](#_nzd3s8kcukic) **38**

[Exemplo](#_dwovn0z9a69n) 39

[**Quais são as actividades do responsável pelo tratamento de dados?**](#_dkrdu7w2g0io) **39**

[**Descreva a finalidade, a pertinência e a obrigatoriedade da avaliação de impacto(AIPD)?**](#_r18idp1dt847) **40**

[**Quais sao as funcoes do DPO?**](#_w5l76izf12ht) **40**

[**O que e considerado dados em grande escala?**](#_czrmswn0yafx) **42**

[CASOS DE OBRIGAÇÃO OU NÃO DE TER EPD](#_1m079j59p0gi) 43

[**Categorias Especiais de Dados Pessoais**](#_qbe91sj8yns3) **44**

[**Transferência de dados pessoais para fora da UE**](#_bo2wh5oyccd0) **45**

[**Quando e que uma empresa esta a cumprir o RGPD**](#_xmfhuw6qjzdp) **45**

# 

# QUESTAO 1

## Justifique e fundamente a conciliação jurídica possível, em caso de colisão, entre os direitos “ao bom nome e reputação” e “à palavra e à imagem” consagrados no n.º 1 do artigo 26º da CRP, e os direitos de “informar, de se informar e de ser informados, sem impedimentos nem discriminações” consagrados no n.º 1 do artigo 37º da CRP.

## **Resposta**

Devem ser conciliados, na medida do possível, os direitos de informação e livre expressão, por um lado, e à integridade moral e ao bom nome e reputação, por outro. II - Quando tal se revele inviável, a colisão desses direitos deve, em princípio, resolver-se pela prevalência daquele direito de personalidade.

A liberdade de informação e de expressão está inscrita no quadro dos direitos, liberdades e garantias pessoais com assento constitucional, assim como em várias declarações internacionais de direitos, e tem por fim último garantir a plenitude da democracia. Não se trata, porém, de um direito absoluto, pois a lei ordinária restringe-a nos casos expressamente previstos na Constituição, limitando-a ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.

Entre os limites à liberdade de expressão encontram-se os direitos da personalidade, mais precisamente, o direito à honra, à privacidade e à imagem, os quais, alicerçados no princípio elementar da dignidade da pessoa humana, são, em regra, absolutos. Este caderno temático concentra todos os sumários dos acórdãos proferidos pelas Secções Cíveis e Criminais tirados entre 2002 e Abril de 2013 a propósito da colisão entre a liberdade de informação e de expressão e os direitos de personalidade e pretende revelar o caminho que a jurisprudência deste Supremo Tribunal de Justiça tem trilhado. Não obstante todo o cuidado colocado na elaboração dos sumários que se seguem, a utilização destes não dispensa a consulta do texto integral da decisão a que os mesmos dizem respeito.

**Artigo 26 - Outros Direitos Pessoais**

1. A todos são reconhecidos os **direitos à identidade pessoal**, ao **desenvolvimento da personalidade**, à **capacidade civil**, à **cidadania**, ao **bom nome** e **reputação**, à **imagem**, à **palavra**, à **reserva da intimidade** **da vida privada** **e familiar** e à **protecção legal contra** quaisquer formas de **discriminação**.
2. A lei estabelecerá garantias efectivas **contra a obtenção e utilização abusivas**, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
3. A lei garantirá a **dignidade pessoal e a identidade genética do ser humano**, nomeadamente na criação, **desenvolvimento e utilização das tecnologias** e na experimentação científica.
4. A privação da cidadania e as restrições à capacidade civil só podem efectuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos.

**Artigo 37-Liberdade de expressão e informação)**

1. Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de se informar, sem impedimentos nem discriminações.
2. O exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura.
3. As infracções cometidas no exercício destes direitos ficarão submetidas ao regime de punição da lei geral, sendo a sua apreciação da competência dos tribunais judiciais.
4. A todas as pessoas, singulares ou colectivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta.

# QUESTAO 2

## No âmbito da Lei do Cibercrime, tipifique os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos, facultando um exemplo de cada uma das tipificações. Fundamente a resposta com a própria lei.

## Resposta

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa

Neste crime, o prejuízo não tem de ser patrimonial, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos.

Artigo 3 falsidadeInformatica

. O crime de falsidade informática previsto no artigo 3º da Lei nº 109/2009 visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informaìticos, de redes e de dados informaìticos.

4.  [Ac. Trib. da Relação do Porto, de 24 de abril de 2013](http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/872f3063233d8de480257b78003e60f3?OpenDocument):- O bem jurídico tutelado pelo crime de falsidade informática (Artigo 3º, nºs 1 e 3 da Lei do Cibercrime),não é o património, mas antes a integridade dos sistemas de informação, através do qual se pretendeimpedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados.

Artigo 6 Acesso ilegítimo

Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

O que é a segurança da informação? É um processo organizado e estruturado que permite preservar a confidencialidade, integridade e a disponibilidade da informação. Confidencialidade é... assegurar que a informação é acessível somente por pessoas devidamente autorizadas. O acesso à informação é restrito a utilizadores legítimos. Integridade é… garantir a veracidade e complementaridade da informação, bem como os seus métodos de processamento. O conteúdo da informação não pode ser modificado de forma inesperada.

Disponibilidade é… assegurar o acesso à informação e bens associados por quem devidamente autorizado. A informação deve estar acessível sempre que necessário.

Quem é o responsável pela segurança da informação? Todos nós somos responsáveis pela segurança da informação e todos temos a responsabilidade de proteger os nossos dados e os que nos são confiados.

No entanto, as organizações possuem pessoas especializadas e dedicadas à segurança da informação e à proteção dos dados pessoais. Estes colaboradores são normalmente designados por CISO - Chefe Information Security Officer ou por DPO - Data Protection Officer. São responsáveis pela proteção da informação contra quebras de confidencialidade, integridade e disponibilidade da mesma.

As principais tarefas do CISO são: Para que esta função tenha sucesso a colaboração e o envolvimento de todos é fundamental. Conto com a tua ajuda! Assim como, sempre que necessitares, o CISO está disponível para te ajudar. Implementar boas práticas de segurança de informação holísticas e estruturadas (Ex. CISO, COBIT, ITIL, etc.); Aplicar, contribuir e rever as normas, políticas e standards de segurança de informação; Executar auditorias e controlos internos regulares; Realizar ações de sensibilização e de formação para os utilizadores; Apoiar a organização e em especial o IT e os gestores de projeto, com foco na segurança; Colaborar na estratégia, desempenho e monitorização do IT.

Para que esta função tenha sucesso a colaboração e o envolvimento de todos é fundamental. Conto com a tua ajuda! Assim como, sempre que necessitares, o CISO está disponível para te ajudar.

# QUESTAO 3

## O Governo português elaborou um projeto de lei que pretende obrigar as instituições públicas e as instituições privadas de solidariedade social (IPSS) a divulgarem o nome dos beneficiários de apoios sociais, de qualquer natureza, através da página de internet da Inspeção Geral de Finanças. Exponha, no seu entendimento, quais os limites legais que esta medida pode enfrentar, e que meios jurídicos tem o Governo para salvaguardar a legalidade constitucional do referido diploma.

## **Resposta**

Regulamento Geral da Proteção de Dados Pessoais (RGPD) e as Instituições Particulares de Solidariedade Social (IPSS)

A 25 de Maio de 2018 surgiu um novo paradigma na proteção de dados pessoais, sob o mote: “A tua vida não te chega”!?

O RGPD vem obrigar as IPSS’s a recolher (tratar) os dados pessoais, estritamente, necessários bem como a mantê-los em segurança.

Conceitos e Definições, Art.º 4.º

**Dados Pessoais:**

Informação relativa a uma pessoa singular viva identificada ou identificável.

É considerada identificável a pessoa singular que possa ser identificada direta ou indiretamente, em especial por referência a um nome, número de identificação, dados de localização ou a elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa singular.

**Titular dos dados:** A pessoa singular viva.

**Categorias especiais de dados:**

São aqueles que revelem a origem racial ou étnica, as opiniões politicas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde, a vida sexual ou a orientação sexual.

Em regra, o tratamento de dados pessoais é proibido, permitindo-se o seu tratamento mediante critérios previamente estabelecidos no RGPD, nomeadamente ao nível da licitude e finalidade, artigo 6.º:

**Licitude**: Obrigação legal; Atribuição legal; Cumprimento de um contrato, consentimento.

**Finalidade**: Cumprir a competência legal, cumprir a atribuição legal, cumprir o contrato (inclui atos pré contratuais), e cumprir o âmbito do consentimento.

Os dados pessoais passam a ser tratadas especificamente para a finalidade que, foram recolhidos não podendo ser utilizados noutras.

Em regra, é proibido o tratamento de dados integrantes da categoria especial.

**Tratamento de dados**: Operação ou conjunto de operações efetuadas sobre dados pessoais, por meios automatizados ou não automatizados (papel), tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

**Responsável pelo tratamento**: A instituição particular de solidariedade social (IPSS).

Encarregado de Proteção de Dados Pessoais: Funciona como interlocutor em relação aos titulares dos dados e também em relação à própria autoridade de controlo (CNPD)

**Autoridade de Controlo**: Comissão Nacional de Proteção de Dados Pessoais.

A problemática do consentimento, artigo 7.º

Ponto essencial: O consentimento só se aplica, quando não houver outros critérios de licitude que, não sejam aplicáveis à situação em concreto.

Pelo que o consentimento deve ser expresso, livre e informado, com direito do titular dos dados em retirá-lo a qualquer momento, bem como restringir o consentimento dado.

A pessoa singular tem por isso o dever de ser informada, de todo o que envolva o tratamento dos seus dados pessoais, nomeadamente a identidade do responsável pelo tratamento (a instituição), o motivo / fundamento pelo qual é solicitado o seu consentimento, por quanto tempo são os seus dados tratados, onde ficam guardados, o encarregado de dados a quem pode recorrer, bem como os seus direitos de apagamento e portabilidade, estes últimos aplicáveis, apenas aos dados tratados por meios automatizados.

Paralelismo do consentimento ao regime de bens de um casamento civil: O consentimento tal como o regime de comunhão de bens adquiridos é supletivo, ou seja, caso não haja outro é aquele que se aplica.

Assim:

Cumpre as IPSS ter o controlo e o comando sobre os dados pessoais que tratam. Garantir a confidencialidade e segurança. Seguindo os princípios da licitude, lealdade, transparência, limitação de finalidades, a minimização dos dados, a exatidão, a limitação de conservação, a integridade e confidencialidade e, por fim a responsabilidade.

As IPSS passam a ter de garantir o cumprimento do RGPD, devendo exigir aos subcontratantes (empresas que fornecem serviços e que, podem, eventualmente, tratar dados cuja a responsabilidade é da IPSS), os mesmos níveis de segurança que a instituição implementou.

A figura do Encarregado de Dados (DPO):

Os artigos 37.º a 39.º do RGPD é referente à figura do encarregado de dados;

Naqueles encontramos:

Muitas Instituições têm procurado informação junto da CNIS acerca do chamado Registo Central do Beneficiário Efectivo, criado como efeito da transposição para a ordem jurídica portuguesa do capítulo III da Directiva da União Europeia nº 2015/849, do Parlamento Europeu e do Conselho, de 20 de Maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou do financiamento do terrorismo, transposição essa efectuada pela Lei nº 89/2017, de 21 de Agosto, que aprovou igualmente o Regime Jurídico do Registo Central do Beneficiário Efectivo, previsto no artº 34º da Lei nº 83/2017, de 18 de Agosto. A questão da aplicabilidade do RCBE às IPSS não é linear. Com efeito, o artº 2º, 1. z) da Lei nº 83/2017, de 18 de Agosto, relativo às “definições” quanto à matéria do diploma, refere-se às «Organização sem fins lucrativos», abrangendo “pessoa coletiva, entidade sem personalidade jurídica ou organização que tem por principal objeto a recolha e a distribuição de fundos para fins caritativos, religiosos, culturais, educacionais, sociais ou fraternais ou outros tipos de obras de beneficência” – o que, em princípio, enquadraria as IPSS. Por outro lado, o artº 5º, b), iii) da mesma Lei 83/2017 qualifica, para os efeitos da referida Lei, e nos termos do Capítulo X, ainda dessa Lei, as “organizações sem fins lucrativos” como “entidades equiparadas a entidades obrigadas” (ao dever de registo).

# QUESTAO 4

## O RGPD visa garantir os direitos dos titulares dos dados pessoais. Descreva quais são os direitos dos titulares de dados, providenciando exemplos de como podem ser colocados em prática. Fundamente a resposta.

## **Resposta**

Neste documento encontra informação mais detalhada sobre os direitos que o Regulamento Geral de Proteção de Dados confere aos titulares dos dados, relativamente aos dados que lhes respeitem e cujo respeito será assegurado pela Universidade Católica Portuguesa na sua relação consigo, na medida em que trate e conserve dados que lhe respeitem no âmbito da sua atividade.

1. [I. Direito de Acesso](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#I.%20Direito%20de%20Acesso)
2. [II. Direito de Retificação](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#II.%20Direito%20de%20Retifica%C3%A7%C3%A3o)
3. [III. Direito ao Apagamento](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#III.%20Direito%20ao%20Apagamento)
4. [IV. Direito à Limitação do Tratamento](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#IV.%20Direito%20%C3%A0%20Limita%C3%A7%C3%A3o%20do%20Tratamento)
5. [V. Direito de Portabilidade](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#V.%20Direito%20de%20Portabilidade)
6. [VI. Direito de Oposição](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#VI.%20Direito%20de%20Oposi%C3%A7%C3%A3o)
7. [VII. Direito a Retirar o seu Consentimento](https://www.ucp.pt/pt-pt/direitos-do-titular-dos-dados#VII.%20Direito%20a%20Retirar%20o%20seu%20Consentimento)

**I. Direito de Acesso**

Sempre que o solicitar, pode obter confirmação sobre se os seus dados pessoais são tratados pela Universidade Católica Portuguesa.

Pode, ainda, aceder aos seus dados pessoais, bem como a obter as seguintes informações:

(I) razões pelas quais os seus dados pessoais são tratados; (II) tipos de dados pessoais que são tratados; (III) entidades a quem os seus dados pessoais podem ser transmitidos, incluindo entidades localizadas em países fora da União Europeia ou organizações internacionais, sendo neste caso informado das garantias aplicadas à transferência dos seus dados; (IV) prazo de conservação dos seus dados ou, se tal não for possível, os critérios para fixar esse prazo; (V) direitos de que goza em relação ao tratamento dos seus dados pessoais; (VI) se os dados pessoais não tiverem sido por si fornecidos, informações sobre a origem dos mesmos; (VII) existência de decisões individuais automatizadas, incluindo definição de perfis, e, nesse caso, informações sobre a lógica subjacente a esse tratamento, bem como sobre a importância e consequências previstas do mesmo.

**III. Direito de Retificação**

Sempre que considerar que os seus dados pessoais (dados pessoais objetivos fornecidos por si) estão incompletos ou incorretos, pode requerer a sua retificação ou que os mesmos sejam completados.

**III. Direito ao Apagamento**

Pode solicitar que os seus dados pessoais sejam apagados quando se verifique uma das seguintes situações:

(I) os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; (II) retire o consentimento em que se baseia o tratamento de dados e não exista outro fundamento jurídico para o mesmo; (III) apresente oposição ao tratamento dos dados e não existam interesses legítimos prevalecentes, a avaliar caso a caso, que justifiquem o tratamento; (IV) os dados pessoais tenham que ser apagados ao abrigo de uma obrigação jurídica a que esteja sujeito a Universidade Católica Portuguesa; ou (V) os dados pessoais tenham sido recolhidos no contexto da oferta de serviços da sociedade de informação.

O direito ao apagamento não se aplica quando o tratamento seja necessário para os seguintes efeitos:

(I) exercício de liberdade de expressão e de informação; (II) cumprimento de obrigação legal que exija o tratamento e que se aplique à Universidade Católica Portuguesa; (III) motivos de interesse público no domínio da saúde pública; (IV) fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, na medida em que o exercício do direito ao apagamento prejudique gravemente a obtenção dos objetivos desse tratamento; ou (V) declaração, exercício ou defesa de um direito num processo judicial.

**IV. Direito à Limitação do Tratamento**

A limitação do tratamento permite ao titular solicitar ao responsável que restrinja o acesso a dados pessoais ou que suspensa as atividades de tratamento. Pode requerer a limitação do tratamento dos seus dados pessoais nos seguintes casos:

(I) se contestar a exatidão dos seus dados pessoais, durante um período de tempo que permita à Universidade Católica Portuguesa verificar a sua exatidão; (II) se a Universidade Católica Portuguesa já não precisar dos dados pessoais para fins de tratamento, mas se esses dados forem necessários para efeitos de declaração, exercício ou defesa de um direito num processo judicial; ou (III) se tiver apresentado oposição ao tratamento, até que se verifique que os interesses legítimos da Universidade Católica Portuguesa prevalecem sobre os seus.

**V. Direito de Portabilidade**

Poderá solicitar à Universidade Católica Portuguesa a entrega, num formato estruturado, de uso corrente e de leitura automática, os dados pessoais por si fornecidos. Tem ainda o direito de pedir que a Universidade Católica Portuguesa transmita esses dados a outro responsável pelo tratamento, desde que tal seja tecnicamente possível. O direito de portabilidade apenas se aplica nos seguintes casos:

(I) quando o tratamento se basear no consentimento expresso ou na execução de um contrato; e (II) quando o tratamento em causa for realizado por meios automatizados.

**VI. Direito de Oposição**

Tem o direito de se opor ao tratamento dos seus dados pessoais a qualquer momento, por motivos relacionados com a sua situação particular, nas seguintes situações:

(I) Quando o tratamento se basear no interesse legítimo da Universidade Católica Portuguesa; ou (II) Quando o tratamento for realizado para fins diversos daqueles para os quais os dados foram recolhidos, mas que sejam compatíveis com os mesmos. A Universidade Católica Portuguesa deixará, nesses casos, de tratar os seus dados pessoais, a não ser que tenha razões legítimas para realizar esse tratamento e que estas que prevaleçam sobre os seus interesses.

Pode também opor‐se ao tratamento dos seus dados para fins de marketing direto, incluindo a definição de perfis que esteja relacionada com esse marketing.

**VII. Direito a Retirar o seu Consentimento**

Nos casos em que o tratamento dos dados seja feito com base no seu consentimento, poderá retirar o consentimento a qualquer momento.

# QUESTAO 5

## Fundamente o princípio jurídico da proteção constitucional dos direitos consagrados no artigo 34º da CRP sobre a correspondência e o sigilo das telecomunicações, e as obrigações do Estado de garantir aos cidadãos um combate eficaz contra o crime organizado e contra o terrorismo. Justifique a resposta ligando estas temáticas ao RGPD.

## **Resposta**

**Artigo 34.º - (Inviolabilidade do domicílio e da correspondência)**

1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.

2. A entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.

3. Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento.

4. É proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal.

1. Correspondência carta postal ou embalagem, assim como meios de comunicação privada, tais como email e todos os suportes digitais são de reserva privada.

2. Mesmo as autoridades para entrar numa propriedade privada precisam de um mandato para isso. Pois não podem invadir propriedade privada sem consentimento e vontade do cidadão proprietário.

Mesmo para entrar numa determinada casa a força com mandato de um juiz terá que ser feito entre as 7 e 22 horas.

3. Fechaduras informáticas, por exemplo, podem levar a um crime também na ordem das ferramentas informáticas. Além de se tratar de um crime de violação de habitação neste caso, acarreta outras agravante

4. Sem um mandato judicial, as autoridades não podem ter acesso à nossa correspondência e telecomunicações

No entanto, o estado tem aumentado o ser poder desta área principalmente em casos de branqueamento de capital, por exemplo. As escutas telefónicas, quando existem suspeitas – uma vez que à legislação que o permite.

O cidadão pode não saber que está a ser escutado, mas autoridades, nomeadamente a tributária possui esse poder.

Enquadramento Legislativo da Proteção de Dados e o Sigilo das Telecomunicações

Em Portugal

O acesso a dados relacionados com as comunicações eletrónicas tem sido uma matéria amplamente regulamentada, algo que se deve, principalmente, a pressões comunitárias (Cf. ponto 10 do Ac. do TC n.º 403/2015). De acordo com o Art. 2.º da CRP a “A República Portuguesa é um Estado de direito democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efectivação dos direitos e liberdades fundamentais e na separação e interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa”. “Na sua vertente de Estado de direito, o princípio de Estado de direito democrático, mais do que constitutivo de preceitos jurídicos, é sobretudo conglobador e integrador de um amplo conjunto de regras e princípios dispersos pelo texto constitucional, que densificam a ideia de sujeição do poder a princípios e regras jurídicas, garantindo aos cidadãos liberdade, igualdade e segurança”. Assim, “Ao Estado incumbe não apenas «respeitar» os direitos e liberdades fundamentais, mas também «garantir a sua efectivação»

Nesta égide importa referir ainda o Art. 34.º, n.º 1 da CRP, pela proteção da inviolabilidade do domicílio e do sigilo da correspondência e dos outros meios de comunicação privada, de forma a que é proibida “toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal” (n.º 4 do mesmo artigo). Importa rever no domínio do Código Civil o seu Art. 70.º, que estabelece que “a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça à sua personalidade física ou moral” e o Art. 80.º – com a epígrafe “Direito à reserva sobre a intimidade da vida privada” – estatui que: “1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem. 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas”.

A União Europeia, ao criar as suas políticas comuns de manutenção do espaço partilhado de liberdade, segurança e justiça, deu azo à criação de um enquadramento jurídico no sentido da proteção dos dados pessoais e para a cooperação entre entidades judiciárias e policiais. O Tratado de Lisboa explicitou que “A União fundase nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem” (Art. 2.º do TFUE).

O Art. 16.º salvaguarda o “direito à proteção dos dados de caráter pessoal”, ao prever que o Parlamento Europeu e o Conselho devem estabelecer “normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados”, conforme o n.º 2

No contexto da Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015 de 20 de fevereiro, e dos desafios instalados pelas novas ameaças à segurança nacional, torna-se urgente o acesso a “meios operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva”, com vista à proteção de um conjunto de garantias presentes na Carta dos Direitos Fundamentais da UE e na Convenção Europeia dos Direitos do Homem. De acordo com a comunicação da Comissão Europeia a propósito da Agenda Europeia para a Segurança8 , “as ameaças estão a tornar-se cada vez mais diversificadas e internacionais, sendo de natureza cada vez mais transnacional e transetorial”, algo que requer “uma resposta eficaz e coordenada a nível europeu”. Neste sentido, é de relevar o facto de a Comissão Europeia observar que “todas as medidas em matéria de segurança têm de respeitar os princípios de necessidade, da proporcionalidade e da legalidade, bem como prever as devidas garantias de responsabilização e de recurso judicial”, indo ao encontro do Art. 52.º, n.º 1 da CDFUE. A

A referida comunicação culmina com a necessidade de aproximação das dimensões interna e externa da segurança, sendo de especial relevo a referência associada à importância dos dados das comunicações, que “podem igualmente ser eficazes para a prevenção e a repressão do terrorismo e da criminalidade organizada”9.

Tratando-se de uma agenda partilhada entre a União e os Estados-Membros na criação de um espaço de segurança interna da UE que exija uma resposta coordenada a nível europeu, com especial incidência em matérias como o terrorismo, a criminalidade organizada e a cibercriminalidade, onde a proteção dos cidadãos seja assegurada em plena conformidade com os direitos, liberdades e garantias fundamentais. 9 A Agenda estabelece três prioridades de atuação, entre as quais, uma resposta forte da UE ao terrorismo e ao fenómeno dos combatentes terroristas estrangeiros, o combate à criminalidade transnacional grave e organizada e a cibercriminalidade – que exigem ação imediata, uma vez que se tratam de domínios claramente interligados de ameaças transnacionais.

As questões relacionadas com a vigilância e privacidade tornaram-se proeminentes nas “information societies” - fortemente dependentes das tecnologias eletrónicas, fomentadas desde de 1970. Desta forma, as tecnologias da informação e comunicação incrementaram não só o desenvolvimento destas sociedades, como incitaram o poder dos sistemas de vigilância das mesmas. Destacando outro período igualmente importante relacionado com a vigilância é de referir o início do século XXI, quando se incentivou a uma resposta internacional concertada ao terrorismo global11 . É certo que ao longo dos últimos anos surgiram novas ameaças, com cada vez maior grau de complexidade e que determinam um reforço concertado das sinergias disponíveis ao seu combate, tornando a cooperação entre países cada vez mais importante. Cumpre referir que contribuiu para a alteração de paradigma um conjunto de acontecimentos que fomentaram o acesso a dados de tráfego, como os atentados terroristas de Madrid (2004) e Londres (2005).

No combate ao terrorismo que se alastrava pela Europa, verificou-se a necessidade de aceder aos dados de tráfego para finalidades de investigação criminal, pelo que devemos considerar a Diretiva de 2006/24/CE, de 15 de março como “legislação de emergência”12. Esta Diretiva previa a obrigação dos fornecedores de serviços de comunicações eletrónicas.conservarem determinados dados, com vista a garantir a disponibilidade destes para efeitos investigação, deteção e repressão de crimes graves (Art. 1.º, n.º 1)

Com vista a fornecer um conjunto mais concreto de operações de tratamento que exigem uma AIPD devido ao elevado risco inerente, tendo em conta os elementos específicos dos artigos 35.º, n.º 1, e 35.º, n.º 3, alíneas a) a c), a lista a adotar a nível nacional nos termos do artigo 35.º, n.º 4, e dos considerandos 71, 75 e 91, e outras referências no RGPD a operações de tratamento «suscetível de implicar um elevado risco»14, devem ser considerados os seguintes nove critérios.

Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados» (considerandos 71 e 91). Os exemplos deste critério podem incluir: uma instituição financeira que faça um controlo seletivo dos seus clientes a partir de uma base de dados de referências de crédito bancário ou a partir de uma base de dados de combate ao branqueamento de capitais e ao financiamento do terrorismo ou de combate à fraude; uma empresa de biotecnologia que ofereça testes genéticos diretamente aos seus clientes por forma a avaliar e prever riscos de doença ou para a saúde; ou uma empresa de desenvolva perfis comportamentais ou publicitários baseados na utilização ou navegação no seu sítio web

# QUESTAO 6

## O RGPD estabelece regras relativamente ao tratamento dos dados pessoais dos candidatos a ofertas de emprego. Elabore um método completo para a obtenção da legitimidade para o tratamento de dados em candidaturas de emprego. Fundamente a resposta.

## **Resposta**

**1. Como gerir os currículos com a nova RGPD?**

Até agora, apenas era necessário o consentimento tácito dos candidatos. Isto é, se um candidato entregava o seu CV se subentendia que este dava permissão para o processamento dos seus dados.

Com o novo regulamento, as empresas necessitam ter o consentimento explícito dos candidatos para o tratamento dos dados do seu currículo. Por isso, é obrigatório que os departamentos de recursos humanos solicitem autorização expressa, seja para os currículos que recebem em formato de papel, através do seu email ou através das redes sociais. Da mesma forma, deve ter a autorização destes para tratar os seus dados se pretende utilizá-los para processos de seleção.

**2. Como solicitar o consentimento explícito dos candidatos?**

Para solicitar a autorização expressa dos candidatos, as empresas devem proporcionar a seguinte informação aos profissionais de modo a poder gerir os seus dados:

* Nome da pessoa responsável pela gestão de dados dos candidatos
* Objetivo da gestão de dados
* Prazo de conservação dos dados
* Direitos dos candidatos sobre o tratamento dos seus dados

Uma vez proporcionada toda a informação, o candidato deve afirmar o seu consentimento de forma clara.

**3. Durante quanto tempo se pode utilizar os dados dos candidatos?**

Pode conservar até um máximo de 2 anos, os dados daqueles candidatos que tenha na sua base de dados. Se o candidato os atualizar, pode continuar a conservar estes dados. Caso contrário, os dados deste devem ser eliminados após 24 meses sem atividade.

**4. Como proceder ao registo da validade dos dados?**

Fazer um seguimento dos currículos que obteve de forma individual, seja em papel ou em formato digital, pode ser bastante complexo. O formato em papel não permite a monitorização dos dados dos candidatos e dificulta a sua gestão quanto à data de caducidade, e como tal pode criar alguns problemas legais.

Por isso, e recomendavel que os dados sejam guardados plataformas digitais ou software especifico da area. Este tipo de sistema será bastante útil, uma vez que, não só permite ter os dados atualizados e controlar a sua validade, como também, gerir os currículos e selecionar os candidatos adequados.

**Recolha e utilização de endereços de email**

Deve ter presente os seguintes conceitos:

* ﻿O **“Opt in”** é a autorização dada por um titular de dados, para receber mensagens de uma determinada instituição.
* O **“Double Opt in”** é um “**Opt in**” reforçado.   
  O Responsável pelo tratamento de dados, após enviar a primeira mensagem, envia uma segunda, geralmente um link, de confirmação. Para que o consentimento seja confirmado, é necessário que o titular dos dados faça a validação do link, ou seja, existe uma dupla confirmação. A validação pode mencionar “por favor confirme a sua subscrição”, sem indicar quaisquer dados adicionais.
* O **“Soft Opt In”** refere-se a uma forma implícita de garantir o envio de comunicações institucionais para os titulares dos dados, uma vez que já exista um relacionamento prévio estabelecido entre as partes. No “Soft Opt in” entende-se que a relação entre as partes já permite o envio de mensagens entre elas.﻿
* O **“Opt out”** aplica-se quando o destinatário indica explicitamente que não deseja receber mensagens de uma lista específica ou global.

# QUESTAO 7

## Quais as obrigações a que está sujeita qualquer empresa ou organização em matéria de proteção de dados pessoais, e que funções estão reservadas à Comissão Nacional de Proteção de Dados. Fundamente a resposta.

## **Resposta**

· **Reforço das obrigações das organizações -** Para além da obrigação de adoção de políticas e procedimentos de segurança de dados, como a pseudonimização ou a cifragem de dados, é criada a figura do Data Protection Officer (DPO) / Encarregado de Proteção de Dados (EPD).

· **Regras especiais para menores -** O RGPD prevê a impossibilidade de menores, com idade inferior a 16 anos, prestarem o seu consentimento para tratamentos de dados em serviços online (oferta direta de serviços da sociedade da informação às crianças), ficando, no entanto, ao critério de cada Estado-membro determinar se os jovens com idades compreendidas entre os 13 e 16 anos poderão ter acesso a serviços online.

· **Obrigação de comunicar quebras de segurança -** As organizações passam a estar obrigadas a notificar os casos de violação de dados pessoais às autoridades competentes e aos próprios titulares dos dados.

· **Accountability -** Desaparece a obrigação de notificação/autorização à CNPD, tornando-se esta um órgão fiscalizador. Há uma mudança de paradigma, que obriga os responsáveis pelo tratamento de dados de serem capazes de, a qualquer momento, demonstrar o cumprimento das exigências previstas no RGPD.

· **Encarregado de Proteção de Dados (EPD) -** As autoridades e organismos públicos estão obrigados a contratar/nomear um EPD, o qual deve ter conhecimentos especializados no domínio do direito e das práticas da proteção de dados, considerando que a sua principal função é controlar o cumprimento das regras do novo Regulamento pela organização.

· **Avaliação de impacto sobre a proteção de dados** - Os tratamentos de dados pessoais suscetíveis de implicar um elevado risco para os direitos e liberdades das pessoas singulares têm de ser precedidos de uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), designadamente nos casos estipulados no nº 3, art. 35º do RGPD e no Regulamento 798/2018, de 30 novembro.

## 

# QUESTAO 8

## O comércio eletrónico é cada vez mais utilizado nas economias modernas. Exponha **quatro direitos** que os consumidores têm para exigirem o integral cumprimento dos contratos que podem celebrar com suporte em plataformas eletrónicas, nomeadamente no que respeita às garantias de equipamentos ou sobre a qualidade dos produtos encomendados a fornecedores com sede em países da União Europeia. Justifique a resposta, com base na Lei do Comércio Eletrónico.

## **Resposta**

Se vender um artigo ou um serviço em linha ou por outro meio de venda à distância (venda por telefone ou por correspondência) ou fora de um estabelecimento comercial (venda porta a porta), o consumidor tem o direito de devolver o artigo ou de anular o serviço no prazo de 14 dias. É o chamado período de reflexão ou de retratação. O consumidor não tem de dar qualquer razão ou justificação.

Ao abrigo da legislação europeia, os consumidores têm direito a uma garantia mínima de dois anos (garantia legal) que lhes assegura uma proteção contra produtos defeituosos, que não sejam conformes com a descrição do vendedor ou que não correspondam ao publicitado. Em alguns países, a legislação nacional pode exigir ao vendedor um período de garantia mais longo.

Se, durante o período de garantia legal, o produto vendido se revelar defeituoso ou não tiver a aparência ou não funcionar como publicitado, o vendedor é responsável. Em alguns países, essa responsabilidade também pode recair sobre o fabricante ou importador.

Na maioria dos países existe uma «hierarquia de meios de reparação». Isto significa que o cliente deve, em primeiro lugar, solicitar a reparação do produto ou a sua substituição se a reparação do mesmo não for uma opção viável (por exemplo, se for demasiado caro). O vendedor deve reparar ou substituir o produto num prazo razoável e sem grandes inconvenientes para o cliente.

# QUESTAO 9

## Os colaboradores das empresas são também titulares de dados pessoais. Descreva em detalhe que ações deverá efetuar o empregador para que se cumpra o RGPD relativamente a estes dados. Fundamente a resposta.

## **Resposta**

Os dados pessoais dos trabalhadores, constantes do seu contrato de trabalho, bem como aqueles que foram transmitidos no decurso da execução daquele, podem ser tratados e incorporados em distintos ficheiros com diversas finalidades: (varios exemplos, escolher alguns)

* processar os salários, gratificações, subsídios e outras vantagens patrimoniais;
* gerir a relação laboral, nomeadamente, a antiguidade, o dossier disciplinar, a carreira contributiva;
* gerir o sistema de higiene, saúde, segurança no trabalho e prevenção de riscos laborais;
* controlar a pontualidade e assiduidade; garantir a segurança das instalações através da gravação de imagens pelo sistema de vídeo vigilância, entre outros.

A Lei impõe expressamente que os dados pessoais dos trabalhadores recolhidos através de meios tecnológicos de vigilância à distância (tais como imagens recolhidas através de câmaras de videovigilância) só possam ser utilizados em procedimento disciplinar se o forem no âmbito de procedimento criminal.

O tratamento dos dados pessoais dos trabalhadores destina-se, essencialmente, a permitir a execução dos contratos de trabalho, assim como para o cumprimento de obrigações legais do empregador e/ou para satisfação de interesses legítimos desta.

O n.º 6 do artigo 28.º da Lei n.º 58/2019 veio legitimar o tratamento dos dados biométricos dos trabalhadores (como sejam a impressão digital, a íris, entre outros) exclusivamente para fins de controlo de acesso às instalações da entidade empregadora ou para fins de controlo de assiduidade dos trabalhadores, devendo assegurar-se que apenas se utilizem representações dos dados biométricos,

O empregador, enquanto responsável pelo tratamento dos dados, está obrigado a aplicar, em permanência, medidas técnicas, organizativas e de controlo, adequadas e permanentes, para assegurar o necessário nível de segurança ao risco, por forma a manter a integridade e a confidencialidade dos dados pessoais conservados e/ou transmitidos, garantindo que as pessoas autorizadas ao tratamento dos dados assumiram uma obrigação contratual de confidencialidade ou a ela estão legalmente sujeitas.

Depois, o trabalhador tem ainda o direito de solicitar ao empregador o acesso aos seus dados pessoais, podendo/devendo proceder à sua retificação, quando incorretos.

Mais, tem o direito à limitação do tratamento dos dados e à sua portabilidade, quando solicitada, assim como o direito ao apagamento dos mesmos.

# QUESTAO 10

## Exponha dois instrumentos jurídicos a que pode recorrer um criador de software de jogos de diversão para salvaguardar os seus direitos de propriedade intelectual, quando presta serviços a uma empresa na condição de trabalhador dependente. Fundamente a resposta com dois exemplos práticos, e com os correspondentes instrumentos legais.

## **Resposta**

**O que é o direito de autor?**

É o ramo do Direito que regula a proteção das obras intelectuais. Traduz-se num conjunto de autorizações de utilização das obras, reservadas ao autor ou a terceiro detentor dos direitos (por ex: herdeiros).

O direito de autor pertence, assim, ao criador intelectual da obra, a menos que haja disposição expressa em contrário e é reconhecido independentemente do registo, depósito ou qualquer outra formalidade.

Nos termos do Código de Direito de Autor e dos Direitos Conexos “Consideram-se obras as criações intelectuais do domínio literário, científico e artístico, por qualquer modo exteriorizadas…”.

O Direito de Autor confere aos titulares de criações intelectuais do domínio literário, científico e artístico, o exclusivo direito de dispor da sua obra e utilizá-la, ou autorizar a sua utilização por parte de terceiros, total ou parcialmente.

A compra de um trabalho protegido por direitos de autor não dá o direito de transmitir ou copiá-lo. Mesmo no uso privado, este nunca deverá atingir a exploração normal da obra, nem causar prejuízo injustificado dos interesses legítimos do autor.

**Designa-se por Propriedade Intelectual** o conjunto de todas as criações do espírito humano, tais como invenções e todo o tipo de soluções técnicas, sinais distintivos, criações estéticas ou obras artísticas e literárias. A propriedade Intelectual opera uma tradicional divisão quanto ao âmbito de criações a tutelar.

Como ponto de partida há que se ter em conta que o software, na União Europeia, não é protegido por patente ou por uma forma especial de proteção, como por vezes se ouve em discussões sobre o tema. Muito se debateu acerca dessas duas possibilidades. No entanto, a Directiva 91/250/CEE de 14 de Maio, relativa à proteção jurídica dos programas de computador, impôs que proteção do software na União Europeia seja feita pelo Direito de Autor (Copyright Approach), nos mesmos termos que as obras literárias

**Direitos autor**

* Encontra-se regulado em Portugal no Código do Direito de Autor e dos Direitos Conexos (DecretoLei N.º 63/85, de 14 de março);
* Divide-se em duas modalidades: Direitos Morais e Direitos Patrimoniais;
* Tem uma duração de 70 anos a contar da morte do autor;
* Não carece de registo para ser reconhecido (podendo, contudo, ser realizado um registo na Inspeção Geral das Atividades Culturais (IGAC) para efeitos de prova desse direito).

**Direitos Conexos**

* Visam proteger as prestações dos artistas intérpretes ou executantes, dos produtores de fonogramas e de videogramas e dos organismos de radiodifusão;
* Têm uma duração de 50 anos contados a partir de uma comunicação licita ao público ou da publicação da prestação artística protegida.

Codigo direitos de autor e direitos conexos:

A resposta encontra-se no Código do Direito de Autor e Direitos Conexos (CDA), aprovado pelo DL n.º 63/85, de 14/3

➢ Regra: O direito de autor pertence ao criador intelectual da obra, salvo disposição expressa em contrário (art. 11.º) • Mas no contrato de trabalho (art. 14.º)

➢ Determina-se de harmonia com o que tiver sido convencionado (n.º 1)

➢ Na falta de convenção: presume-se que o direito de autor pertence ao seu criador intelectual (n.º 2)

➢ Não sendo o nome do criador mencionado, vigora a presunção contrária: o direito de autor é do empregador - esta última presunção pode ser ilidida caso o criador venha a revelar a sua identidade (art. 30.º n.º 2 - Direito irrenunciável de o autor revelar em qualquer altura a sua identidade e a autoria da obra)

Para que o direito de autor seja atribuído ao empregador, é necessário que:

➢ A prestação laboral contratada tenha por objeto a criação de uma ou mais obras intelectuais pelo trabalhador – à obra criada acidentalmente não se aplica o regime, sendo necessário que a criação se dê em cumprimento do contrato de trabalho

➢ O género da obra intelectual criada se integre no objeto da prestação laboral contratada ➢ A utilização se contenha no âmbito do convencionado ou consentido pelo trabalhador

Sempre que a titularidade do direito de autor pertença ao empregador, o trabalhador criador pode exigir uma remuneração especial para além da ajustada:

➢ Quando a criação intelectual exceda claramente o desempenho zeloso da função que lhe estava confiada (n.º 4 alínea a));

➢ Quando da obra vierem a fazer-se utilizações ou a retirar-se vantagens não previstas na fixação da remuneração ajustada (n.º 4 alínea b)) • Pertencendo o direito de autor por convenção ao trabalhador criador:

➢ A obra apenas pode ser utilizada para os fins previstos na convenção (art. 15.º n.º 1)

➢ O trabalhador criador não pode fazer utilização da obra que prejudique os fins para que foi produzida (art. 15.º n.º 3) – na ausência de convenção, correspondem à atividade principal do empregador

1 - Nos casos dos artigos 13.º e 14.º, quando o direito de autor pertença ao criador intelectual, a obra apenas pode ser utilizada para os fins previstos na respectiva convenção.

2 - A faculdade de introduzir modificações na obra depende do acordo expresso do seu criador e só pode exercer-se nos termos convencionados.

3 - O criador intelectual não pode fazer utilização da obra que prejudique a obtenção dos fins para que foi produzida.

Aquele que subsidie ou financie por qualquer forma, total ou parcialmente, a preparação, conclusão, divulgação ou publicação de uma obra não adquire por esse facto sobre esta, salvo convenção escrita em contrário, qualquer dos poderes incluídos no direito de autor.

# QUESTAO 11

## Os direitos à liberdade de expressão e de informação não são absolutos, e têm de ser conciliados com outros direitos de igual relevância constitucional. Justifique como conciliar os direitos dos jornalistas à publicação de notícias de relevante interesse público, e os direitos à reserva da vida privada e familiar de figuras públicas que desempenham cargos políticos. Justifique a resposta com os normativos constitucionais aplicáveis.

## **Resposta**

A liberdade de imprensa abrange o direito de informar, de se informar e de ser informado, sem impedimentos nem discriminações. Todos têm o direito à reserva da intimidade da sua vida privada e familiar, sendo certo que a extensão de tal reserva depende da natureza do caso e da condição das pessoas.

A natureza do caso tem a ver com os factos concretos que estiverem em causa. A condição das pessoas reporta-se às pessoas em concreto, já que varia bastante a reserva da vida privada que cada pessoa entende ser-lhe devida e que deve ser respeitada.

Existem pessoas que têm um direito de reserva da sua vida privada mais reduzido do que o comum das pessoas, em virtude das suas funções ou notoriedade. As figuras públicas — dado o interesse público em as conhecer melhor ou de uma forma mais completa, seja por que são políticos ou figuras da administração pública ou porque buscaram a notoriedade e gozam dos benefícios da mesma.

Figuras públicas que não detenham responsabilidades políticas e administrativas, isto é, que não sejam titulares de cargo públicos, tais como artistas ou figuras "mediáticas" diversas, a justificação para a redução da reserva da sua vida privada tem sido encontrada no facto de essas figuras usarem, muitas vezes, a sua vida privada para fins publicitários e comerciais, vivendo numa quase permanente exposição mediática de onde retiram vantagens diversas.

O interesse público legítimo relevante reporta-se sempre a valores de ordem social numa sociedade democrática, afastando como justificação da violação da reserva da vida privada a mera curiosidade, o interesse mórbido ou sensacionalista, ou mesmo um interesse social pouco relevante.

No entanto, quem divulgar factos da vida privada de outrem não será punido quando a divulgação seja realizada como meio adequado a interesse público legítimo e relevante.

3. Direitos e deveres dos jornalistas

Os direitos dos jornalistas encontram-se plasmados no Capítulo I do Título II da Parte I da CRP, relativo aos Direitos, Liberdades e Garantias Pessoais, concretamente no artigo 37.º, que consagra a liberdade de expressão e o direito de informação em geral, no artigo 38.º, que se ocupa da dimensão institucional dessas liberdades, no artigo 39.º, que prevê a estrutura organizativa de garantia desses direitos, e, por fim, no artigo 40.º, que se debruça sobre as formas específicas de expressão e informação (49). No seu conjunto, estes direitos

Enquanto a liberdade de expressão e os direitos de se informar e de ser informado são individuais, o direito de informar tanto pode ser individual como institucional. Por seu turno, a liberdade de comunicação social é, necessariamente, institucional uma vez que “pressupõe organização (e organização de empresa), ainda que dependa sempre de actividade de pessoas individualmente consideradas (os jornalistas, os colaboradores, e até os leitores, os ouvintes, os telespectadores)

O direito de expressão, ínsito no n.º 1 do artigo 37.º da CRP, é, desde logo, a liberdade de expressão e de pensamento, que engloba: “(i) o direito de não ser impedido de se exprimir e de divulgar, pelos meios a que se tenha acesso, ideias e opiniões; (ii) a liberdade de comunicar ou não comunicar o seu pensamento; (iii) uma pretensão à expressão, através da remoção de obstáculos não-razoáveis no acesso aos diversos meios (…); (iv) uma pretensão a alguma medida de acesso, em termos a configurar por lei, às estruturas de serviço público de rádio e de televisão; (v) pretensões de protecção contra ofensas provenientes de terceiros” (53). Este direito, a par da liberdade de criação, encontra-se consagrado, ainda, na al. a) do artigo 6.º e no artigo 7.º do Estatuto do Jornalista, aprovado pela Lei n.º 1/99, de 1 de Janeiro.

Todavia, “«sem impedimentos» não pode querer dizer sem limites” (54). Um desses limites passa pelo “controlo da verdade pelos jornalistas [que] se deve reportar às declarações difundidas por terceiros” (55). Outro desses limites tem que ver com possíveis infrações cometidas no exercício da liberdade de expressão e de informação em prejuízo de outros direitos constitucionais que com ele colidam, o que pode gerar, em função da sua gravidade, responsabilidade criminal ou contraordenacional (vide o n.º 3 do artigo 37.º da CRP).

Preceitua, ainda, o n.º 2 daquele normativo que a liberdade de expressão e informação e a liberdade de imprensa não podem ser impedidas no seu exercício ou limitadas por qualquer forma de censura (56). Por último, o n.º 4 do mesmo artigo refere-se ao direito de resposta e de retificação, enquanto “instrumento de defesa das pessoas contra qualquer opinião ou imputação de carácter pessoal ofensiva ou prejudicial” (57).

# Questao 12

## A concentração excessiva dos capitais das empresas de media e o cruzamento de capitais entre grupos com os mesmos sócios ou acionistas é proibida na Constituição da República Portuguesa. Faça o enquadramento jurídico dessa questão, quer ao nível da CRP, quer ao nível da Lei da Imprensa, relevando ainda as funções que cabem à ERC nesta mesma matéria. Fundamente a resposta identificando e transcrevendo os preceitos legais aplicáveis.

A concentração excessiva dos capitais das empresas de media e o cruzamento de capitais entre grupos com os mesmos sócios ou acionistas é proibida na Constituição da República Portuguesa. Faça o enquadramento jurídico dessa questão, quer ao nível da CRP, quer ao nível da Lei da Imprensa, relevando ainda as funções que cabem à ERC nesta mesma matéria. Fundamente a resposta identificando e transcrevendo os preceitos legais aplicáveis.

No que diz respeito ao quadro jurídico, existem várias regras específicas e algumas de âmbito mais geral que permitem dar cumprimento ao pluralismo no sector dos media. Portugal tem, uma entidade reguladora ERC que monitoriza as questões-chave do sector da comunicação social, designadamente, a questão da transparência da propriedade, o pluralismo dos media, o Public Service Media (RTP), isto é, o sector público da televisão e da rádio, fazendo-o, nomeadamente, através de auditorias, relatórios, pareceres e vários estudos aplicados ao sector.

Esta autoridade tem as suas próprias garantias de independência, bem como as suas incompatibilidades bem especificadas, o que lhe confere a capacidade de exercer as suas competências com imparcialidade e transparência.

No entanto, para reforçar a sua independência, estamos de acordo com algumas opiniões e setores da sociedade portuguesa que acreditam que é importante que os membros das entidades reguladoras também possam ser indicados e / ou nomeados pelo Presidente da República, de forma a melhorar a garantir uma maior independência dos sistemas de regulação em Portugal

De referir ainda uma outra entidade de regulação. Em Portugal, a AdC - Autoridade da Concorrência, tem poderes transversais de regulação sobre a economia portuguesa para a aplicação das regras de concorrência, nomeadamente no que respeita à concentração dos media, em coordenação com a regulação sectorial, neste caso a ERC. Há garantias constitucionais ou legais explícitas e salvaguardas regulamentares para a independência da Autoridade da Concorrência, bem como da Autoridade de Telecomunicações –Anacom (que regula o sector das telecomunicações e comunicações eletrónicas), de qualquer interferência política ou comercial. E das decisões destas autoridades, existem naturalmente mecanismos de recurso eficazes em vigor

Existem ainda alguns problemas com a implementação eficaz das salvaguardas regulamentares relativamente às questões de propriedade dos media e / ou de controlo dos meios de comunicação por parte de agentes políticos. A lei contém limitações à participação direta e indireta excessiva e / ou ao controlo de redes de televisão por partidos políticos, grupos partidários ou agentes políticos, mas em relação à transparência da propriedade no sector da comunicação social, em alguns casos, torna-se muito difícil saber exatamente 9 António Marinho e Pinto, “Mais do mesmo”. Expresso, 15 de agosto de 2015. 111 quem são os proprietários dos meios de comunicação social portugueses. É difícil obter conhecimento cabal dos verdadeiros proprietários de alguns grupos de media, isto porque, por vezes o que é apresentado como sendo os detentores do capital são fundos de investimento muito provavelmente sedeados em offshores. Por exemplo, atualmente, não é possível identificar a estrutura acionista do grupo de media Português Newshold. Para ultrapassar este problema uma nova lei sobre a transparência da propriedade, gestão e financiamento dos órgãos de comunicação social foi aprovada pelo Parlamento em 2 de julho de 2015. Com exceção deste problema, não há risco significativo em Portugal de filiações políticas dos media, por assim dizer, e de controlo direto por parte do sistema político dos meios de comunicação e respetivas redes de distribuição.

**CRP**

# **Decreto de aprovação da Constituição**

Artigo 39 do CRP regulação da comunicação social

1. Cabe a uma entidade administrativa independente assegurar nos meios de comunicação social:

a) O direito à informação e a liberdade de imprensa;

b) A não concentração da titularidade dos meios de comunicação social;

c) A independência perante o poder político e o poder económico;

d) O respeito pelos direitos, liberdades e garantias pessoais;

e) O respeito pelas normas reguladoras das actividades de comunicação social;

f) A possibilidade de expressão e confronto das diversas correntes de opinião;

g) O exercício dos direitos de antena, de resposta e de réplica política.

2. A lei define a composição, as competências, a organização e o funcionamento da entidade referida no número anterior, bem como o estatuto dos respectivos membros, designados pela Assembleia da República e por cooptação destes.

# **Decreto de aprovação da Constituição**

**ERC**

**São atribuições da ERC no domínio da comunicação social:**

b) Velar pela não concentração da titularidade das entidades que prosseguem actividades de comunicação social com vista à salvaguarda do pluralismo e da diversidade, sem prejuízo das competências expressamente atribuídas por lei à Autoridade da Concorrência;

c) Zelar pela independência das entidades que prosseguem actividades de comunicação social perante os poderes político e económico;

# Questao 13

## O Estatuto do Jornalista, enquanto lei da República, estabelece deveres muito concretos aos profissionais do setor. Identifique esses mesmos deveres, fazendo um estudo comparativo entre eles e os mesmos preceitos consagrados no Código Deontológico o Jornalista. Fundamente a resposta com a transcrição dos referidos deveres nos dois instrumentos jurídicos.

Artigo 14.º

Deveres

1 - Constitui dever fundamental dos jornalistas exercer a respectiva actividade com respeito pela ética profissional, competindo-lhes, designadamente:

a) Informar com rigor e isenção, rejeitando o sensacionalismo e demarcando claramente os factos da opinião;

b) Repudiar a censura ou outras formas ilegítimas de limitação da liberdade de expressão e do direito de informar, bem como divulgar as condutas atentatórias do exercício destes direitos;

c) Recusar funções ou tarefas susceptíveis de comprometer a sua independência e integridade profissional;

d) Respeitar a orientação e os objectivos definidos no estatuto editorial do órgão de comunicação social para que trabalhem;

e) Procurar a diversificação das suas fontes de informação e ouvir as partes com interesses atendíveis nos casos de que se ocupem;

f) Identificar, como regra, as suas fontes de informação, e atribuir as opiniões recolhidas aos respectivos autores.

2 - São ainda deveres dos jornalistas:

a) Proteger a confidencialidade das fontes de informação na medida do exigível em cada situação, tendo em conta o disposto no artigo 11.º, excepto se os tentarem usar para obter benefícios ilegítimos ou para veicular informações falsas;

b) Proceder à rectificação das incorrecções ou imprecisões que lhes sejam imputáveis;

c) Abster-se de formular acusações sem provas e respeitar a presunção de inocência;

d) Abster-se de recolher declarações ou imagens que atinjam a dignidade das pessoas através da exploração da sua vulnerabilidade psicológica, emocional ou física;

e) Não tratar discriminatoriamente as pessoas, designadamente em razão da ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual;

f) Não recolher imagens e sons com o recurso a meios não autorizados a não ser que se verifique um estado de necessidade para a segurança das pessoas envolvidas e o interesse público o justifique;

g) Não identificar, directa ou indirectamente, as vítimas de crimes contra a liberdade e autodeterminação sexual, contra a honra ou contra a reserva da vida privada até à audiência de julgamento, e para além dela, se o ofendido for menor de 16 anos, bem como os menores que tiverem sido objecto de medidas tutelares sancionatórias;

h) Preservar, salvo razões de incontestável interesse público, a reserva da intimidade, bem como respeitar a privacidade de acordo com a natureza do caso e a condição das pessoas;

i) Identificar-se, salvo razões de manifesto interesse público, como jornalista e não encenar ou falsificar situações com o intuito de abusar da boa fé do público;

j) Não utilizar ou apresentar como sua qualquer criação ou prestação alheia;

l) Abster-se de participar no tratamento ou apresentação de materiais lúdicos, designadamente concursos ou passatempos, e de televotos.

3 - Sem prejuízo da responsabilidade criminal ou civil que ao caso couber nos termos gerais, a violação da componente deontológica dos deveres referidos no número anterior apenas pode dar lugar ao regime de responsabilidade disciplinar previsto na presente lei.

**Código deontológico jornalista**

1. O jornalista deve relatar os factos com rigor e exatidão e interpretá-los com honestidade. Os factos devem ser comprovados, ouvindo as partes com interesses atendíveis no caso. A distinção entre notícia e opinião deve ficar bem clara aos olhos do público.

2. O jornalista deve combater a censura e o sensacionalismo e considerar a acusação sem provas e o plágio como graves faltas profissionais.

3. O jornalista deve lutar contra as restrições no acesso às fontes de informação e as tentativas de limitar a liberdade de expressão e o direito de informar. É obrigação do jornalista divulgar as ofensas a estes direitos.

4. O jornalista deve utilizar meios leais para obter informações, imagens ou documentos e proibir-se de abusar da boa-fé de quem quer que seja. A identificação como jornalista é a regra e outros processos só podem justificar-se por razões de incontestável interesse público e depois de verificada a impossibilidade de obtenção de informação relevante pelos processos normais.

5. O jornalista deve assumir a responsabilidade por todos os seus trabalhos e atos profissionais, assim como promover a pronta retificação das informações que se revelem inexatas ou falsas.

6. O jornalista deve recusar as práticas jornalísticas que violentem a sua consciência.

7. O jornalista deve usar como critério fundamental a identificação das fontes. O jornalista não deve revelar, mesmo em juízo, as suas fontes confidenciais de informação, nem desrespeitar os compromissos assumidos, exceto se o usarem para canalizar informações falsas. As opiniões devem ser sempre atribuídas.

8. O jornalista deve salvaguardar a presunção de inocência dos arguidos até a sentença transitar em julgado. O jornalista não deve identificar, direta ou indiretamente, as vítimas de crimes sexuais. O jornalista não deve identificar, direta ou indiretamente, menores, sejam fontes, sejam testemunhas de factos noticiosos, sejam vítimas ou autores de atos que a lei qualifica como crime. O jornalista deve proibir-se de humilhar as pessoas ou perturbar a sua dor.”

9. O jornalista deve rejeitar o tratamento discriminatório das pessoas em função da ascendência, cor, etnia, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social, idade, sexo, género ou orientação sexual.

10. O jornalista deve respeitar a privacidade dos cidadãos exceto quando estiver em causa o interesse público ou a conduta do indivíduo contradiga, manifestamente, valores e princípios que publicamente defende. O jornalista obriga-se, antes de recolher declarações e imagens, a atender às condições de serenidade, liberdade, dignidade e responsabilidade das pessoas envolvidas.

11. O jornalista deve recusar funções, tarefas e benefícios suscetíveis de comprometer o seu estatuto de independência e a sua integridade profissional. O jornalista não deve valer-se da sua condição profissional para noticiar assuntos em que tenha interesse.

# Video TEDX Conclusao

Durante a última década, algumas das empresas mais bem-sucedidas do mundo enriqueceram através dos dados de utilizadores e vendendo-os a empresas de publicidades.

A grande questão é se isto continuará a ser um modelo de negócios sustentável com o exame cada vez maior sobre privacidade de dados e, se não, qual é a alternativa?

Muitos dizem que o escândalo da Cambridge Analytica trouxe à tona as maneiras pelas quais algumas empresas estavam a monetizando dados pessoais sobre seus utilizadores.

Como resultado, o Facebook recebeu recentemente uma multa de US $ 5 bilhões e novas verificações de privacidade após uma investigação de um ano pelos órgãos reguladores dos EUA sobre o escândalo da Cambridge Analytica e outras violações da privacidade de dados.

Este não é um problema exclusivo dos gigantes do Silicon Valley. Na Europa, multas pesadas também foram recentemente distribuídas à British Airways e à Marriott por violações de dados. Como as reclamações sobre proteção de dados dobraram ano a ano, os reguladores estão ficando mais exigentes com as empresas para garantir sua conformidade com o RGPD (Regulamento Geral de Proteção de Dados).

Enquanto isso, o RGPD conduziu um movimento global, já que governos fora da UE, da Austrália ao Brasil, devem introduzir regulamentos semelhantes de proteção de dados. A política do RGPD ajudou a criar maior conscientização sobre a proteção de dados entre as massas.

A convergência de uma cultura de conformidade nas organizações, regulamentações mais rígidas de privacidade de dados em todo o mundo e os consumidores cada vez mais conscientes de seus direitos continuarão a ter um enorme impacto nas empresas que lucram com dados pessoais e até em qualquer empresa que os colete.

AUMENTAR DADOS AO MAXIMIZAR A PRIVACIDADE

Melhor privacidade para indivíduos não significa que é mau para os negócios. Pelo contrário, as empresas podem usar essa oportunidade para estabelecer confiança com os clientes, ao mesmo tempo em que se tornam mais atenciosas e inovadoras quanto à sua abordagem à monetização de dados.

Aqui estão os três principais fatores que as organizações precisam saber sobre como monetizar seus dados, respeitando a privacidade e cumprindo os regulamentos:

-Para muitas empresas, a monetização de dados tem sido inextricavelmente vinculada aos dados pessoais de seus clientes. No entanto, eles podem coletar, gerar ou arquivar outros tipos de dados não pessoais que podem ser valiosos para determinados usuários finais. Ou seja, os dados alternativos que podem até ser esquecidos pela empresa que os trata.

De fato, existem muitos casos de uso para esses dados alternativos no mundo dos investimentos, quando todas as informações oportunas ajudam a ganhar vantagem. É aqui que os dados anonimizados e agregados são mais importantes e as informações de identificação pessoal têm valor zero. O que mais importa para economistas e gerentes de ativos é quantos refrigerantes a Coca Cola está vendendo na Europa neste trimestre, e não se John Doe comprou uma Coca-Cola. O foco nunca é sobre quem, mas o quê e quanto.

-A maioria das empresas possui mais dados do que sabem com o que fazer. A Forrester relatou que, em média, entre 60% a 73% de todos os dados em uma empresa não são utilizados. Porém, novas ferramentas e tecnologias tornaram mais fácil extrair e processar grandes quantidades de dados brutos em insights. Essas ideias podem servir como informações oportunas para aqueles em outros setores, como economistas, analistas ou investidores, procurando identificar padrões e tendências.

Dados valiosos ou perspicazes são simplesmente dados de boa qualidade. E embora os dados sejam sempre descritos como um dos ativos corporativos mais valiosos, geralmente não são tratados como um. Para que as empresas possam liberar todo o poder dos dados, precisam abordá-los com o máximo cuidado possível. Eles precisarão considerar cuidadosamente questões como gerenciamento da arquitetura de dados e gerenciamento da qualidade dos dados. Se os dados não são o principal negócio, eles precisam encontrar os parceiros de tecnologia certos para garantir que eles atendam aos padrões que permitem a geração de insights.

-Os dados brutos de uma empresa por si só podem ser unidimensionais. Mas a integração de dados de diferentes empresas e setores pode fornecer uma imagem mais completa e diferenciada.

Por exemplo, uma empresa que trabalha com fornecedores de todo o país pode ter dados sobre as vendas nacionais de bebidas. Ele poderia rastrear essas vendas e fornecer informações adicionais aos fornecedores como um valor agregado para ajudá-los a melhorar as vendas e as promoções. A empresa também pode compartilhar esses dados com as marcas de bebidas, para que possam ajustar e otimizar o marketing por cidade. Isso permitiria que a empresa monetizasse seus dados e abrisse um novo fluxo de receita, sem nunca compartilhar informações confidenciais que colocariam em risco seu relacionamento com os clientes.

Quando as informações são fornecidas de forma agregada, é uma maneira segura de fornecer um nível excecional de visão sem comprometer a privacidade. Ele permite que perguntas econômicas, sociais e comerciais sejam respondidas sem revelar os detalhes de qualquer indivíduo.

O foco crescente na privacidade não significa que a monetização dos dados tenha sido retirada da mesa. Os dados sempre serão um ativo importante e valioso para qualquer organização, mas precisam ser aproveitados com o pleno respeito dos direitos individuais à privacidade.

## Comentário Nuno:

Muitas empresas hoje em dia dão a volta á anonimização com estas questão de “cross-reference”

O RGPD recebeu uma atualização, relativamente aos dados pessoais, em que qualquer cruzamento de dados a montante, se o seu consentimento é dado ou não.

Neste momento temos a polícia europeia a multar seriamente esta entidades (como a Google), e mesmo assim continua.

E o mais chocante disto, é que nós temos um valor. Quem tem conta Google, conta facebook, se fazemos compras online, ou utilizamos um serviço como “uber eats” é registado num banco de dados, ou seja, todas as empresas que utilizam publicidade online.

O senhor do vídeo diz um ponto interessante, ter uma aplicação (a sonae já o tem), em que mal deteta o IP, o address do Telemóvel, começa a fazer um tracking da pessoa, e começamos a receber publicidade.

Apoia o principio de não usar a economia partilhada, todas a entidade de economia partilhada, dão todos os nossos dados aos parceiros e sub-parceiros, e por isso quando deixamos de utilizar um serviço, devemos exercer o nosso direito de esquecimento.

O RGPD aparece para colmatar.

# RGPD Perguntas da Aula

## Explique por suas palavras o que e o RGPD

O RGPD define os direitos e obrigações legais relativos à recolha, processamento e circulação de dados pessoais dos cidadãos da UE. Fornece um nível de proteção elevado e coerente, equivalente em todos os Estados Membros, e é extensível às organizações externas à UE que trabalham com dados pessoais dos cidadãos da UE.

As obrigações relacionadas com a manipulação de dados pessoais abrangem agora situações como o direito a ser esquecido e a obrigatoriedade de informar o regulador no caso de existir uma violação de segurança que possa comprometer o acesso aos dados pessoais por pessoas não autorizadas para o efeito.

## Dos paises da uniao europeia qual e a idade que consideram uma “crianca”

* Inglaterra 13 anos ja nao e considerado crianca
* Geralmente 14 ou < no resto da uniao europeia

Caso proceda ao tratamento de dados pessoais respeitantes a uma criança com base no consentimento, tem de obter o consentimento parental. No entanto, uma vez que o limiar etário varia entre os 13 e os 16 anos nos diferentes países, é aconselhável consultar a legislação nacional.

## O que considera ser dados pessoais?

(ARTIGO 4)

são todos os dados sobre uma pessoa que uma organização recolhe, armazena e transmite: formulários web, cookies, preferências de utilizador, relatórios médicos, recibos de vencimento, etc.. O RGPD reforça o processamento dos dados pessoais de forma legal, justa e transparente em relação à pessoa em causa.

Ao nível legal, no RGPD os dados pessoais são definidos como:

* Informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»);
* é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

(ARTIGO 9) O RGPD leva em consideração tipos especiais de dados altamente sensíveis, como seja informação médica, convicções criminais, vida sexual, orientações políticas, dados genéticos, etc.. Em tais casos, aplicam-se regras especiais.

## A quem se aplica o RGPD?

O RGPD aplica-se a todas as pessoas e organizações que recolham, reúnam, transmitam ou processem de qualquer forma os dados pessoais dos cidadãos da União Europeia. Sim, isso significa que as organizações não pertencentes à UE têm igualmente de cumprir com este regulamento quando tratam dados pessoais de cidadãos da UE.

As micro, pequenas e médias empresas têm níveis de conformidade um pouco mais simplificados. Tal inclui uma derrogação para organizações com menos de 250 colaboradores em relação à manutenção de registos.

As organizações públicas e de direito penal são abrangidas por regras especiais, uma vez que abordam questões específicas de índoles nacionais e europeias.

## Defina as categorias de dados pessoais abrangidos pelo RGPD

É evidente que os requisitos de proteção previstos no RGPD que possam identificar uma pessoa devem ser sempre assegurados, independentemente da tecnologia utilizada para o tratamento em automatização ou manual.

Todos os dados pessoais que sejam considerados anónimos de modo a que a pessoa não seja identificável deixam de ser considerados dados pessoais. Para que os dados sejam anonimizados, deve existir uma relação redirecionada e personalizada por informações adicionais de forma que a pessoa volte a ser identificada ou identificável.

Todos os dados pessoais descaracterizados, codificados ou pseudonimizados, que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD.

**Pode-se compreender como categorias de dados pessoais abrangidos pelo RGPD:**

* **Dados pessoais** (nome, morada, endereço de email, endereço IP, ID de dispositivo);
  + permitem diretamente a identificação do seu titular.
* **Dados pseudo-anónimos** (endereço de email criptografado, ID de usuário);
  + permitem a identificação do seu titular através de informações adicionais.
* **Dados anónimos** (scripts de trilha, ID de rastreio).
  + não deveriam permitir a identificação do seu titular tout court.

## Quais a exigencias do RGPD

## Principios gerais do RGPD

O Responsável pelo Tratamento de Dados tem obrigação de respeitar os seguintes princípios:

1. ﻿﻿Os dados são processados de forma legal, justa e transparente
   1. (“licitude, lealdade e transparência”);
2. Os dados são recolhidos para finalidades determinadas, explícitas e legítimas e não serão tratados posteriormente de forma incompatível com essas finalidades. O tratamento adicional para fins de arquivo de interesse público, pesquisa científica ou histórica ou para fins estatísticos é admissível
   1. (“limitação da finalidade e da conservação”);﻿
3. ﻿Os dados são adequados, pertinentes e limitados ao necessário em relação à finalidade para a qual são tratados
   1. (“minimização de dados”);
4. ﻿Os dados são exatos e, sempre que necessário, atualizados
   1. (“exatidão”);
5. ﻿﻿Os dados não serão conservados durante mais tempo do que o necessário para o efeito
   1. (“limitação da conservação”);
6. ﻿Os dados são tratados de uma maneira que garanta a segurança apropriada, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas
   1. (“integridade e confidencialidade”).

﻿

﻿O princípio da responsabilidade consagrado no n.º 2 do art.º 5.º, em conjugação com o art.º 24.º do RGPD exige, ainda, do Responsável pelo Tratamento de Dados a aplicação de medidas adequadas e eficazes e políticas de proteção de dados com base num critério de risco e de adaptabilidade e proporcionalidade das medidas que garantam o respeito pelos princípios e obrigações do RGPD e, quando solicitado, a sua demonstração às autoridades de controlo.

## Escreva por suas palavras as possíveis medidas de licitude nas operações

**Artigo: 9**

O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

1. O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
   1. **Artigo: 7, 8, 9**
   2. **razão: 32, 42, 43, 171**
2. O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
   1. **Artigo: 20**
3. O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
4. O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
5. O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
6. O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.
   1. **Artigo: 7, 8, 9**
   2. **razão: 32, 42, 43, 171**

**INFORMAÇÃO A BAIXO SÓ NO CASO DE SER NECESSÁRIO**

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

1. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.o 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.
2. O fundamento jurídico para o tratamento referido no n.o 1, alíneas c) e e), é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.o 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.
3. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.o, n.o 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:
   1. **Artigo: 5, 13, 14**
   2. **razão: 50**
4. Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
5. O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
6. A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.o, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.o;
7. As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
8. A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

## Descreva por suas palavras o que é a accountability

Este princípio é o da responsabilização das pessoas encarregadas de um tratamento de dados pessoais. Cada empresa deve avaliar a sua política e a gestão dos riscos envolvidos para preparar as respostas adequadas.

* O que fazer em caso de ataques cibernéticos, de roubos de dados ou de hacking?
* Como é que os seus dados passam pelos seus serviços e quem pode ter acesso a eles?
* O que faz para os proteger, respeitando a confidencialidade e certificando-se de que os pedidos de supressão ou de alteração estão bem implementados?

Este trabalho de responsabilização comum e global exige o envolvimento de todas as partes interessadas da empresa, que devem ser coordenadas por um piloto, responsável pela missão ou representante na pessoa de um Encarregado de Proteção de Dados (geralmente chamado “DPO” para Data Privacy Officer). É impossível abdicar das políticas internas ou dos antigos processos. A partir do momento em que implementa tratamentos de dados pessoais para prosseguir um objetivo específico (exemplo: recolha de dados para uma campanha de emailing), torna-se responsável e deve ser capaz de responder perante a CNIL acerca das medidas implementadas, no âmbito da proteção e segurança dos dados tratados.

## Qual e a diferenca entre o accountability, a prova e evidência do cumprimento e a licitude nas operações

**Prova e Evidência de Cumprimento (Accountability)**

O regulamento exige que os responsáveis pelo tratamento apliquem medidas adequadas para assegurar e comprovar

Um cliente perguntou-me: “Accountability é para fazer o quê?” – Pois, é…muito trabalhinho! O Regulamento Geral de Proteção de Dados (RGPD) exige que seja implementado um programa de conformidade capaz de monitorizar a conformidade em toda a organização e demonstrar às autoridades de proteção de dados e aos titulares dos dados que todos os dados pessoais estão em segurança. Identifiquei 39 artigos sob o RGPD que exigem a evidência de uma medida técnica ou organizacional para demonstrar a conformidade. Daqui podem ser mapeadas

O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

=> Artigo: 9

a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

=> Artigo: 7, 8, 9

=> razão: 32, 42, 43, 171

b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

=> Artigo: 20

c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

=> Artigo: 13, 21

=> razão: 113, 47, 48

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

## Descreve por suas palavras os novos direitos, indicando como podem ser exercidos e que penalizações poderao existir para quem nao os comprir

**fornecer informações transparentes**

* as empresas devem fornecer aos indivíduos informações sobre quem efetua o tratamento, de quê e porquê.

**direito de acesso e direito à portabilidade dos dados**

* Os indivíduos têm o direito de solicitar acesso aos dados pessoais que lhes digam respeito, gratuitamente e num formato acessível.

**direito ao apagamento (direito a ser esquecido)**

* Em determinadas circunstâncias, um indivíduo pode pedir que o responsável pelo tratamento apague os seus dados pessoais, nomeadamente quando esses dados já não são necessários para cumprir a finalidade do tratamento.
* No entanto, a sua empresa não é obrigada a atender o pedido de um indivíduo se:
  + o tratamento for necessário para respeitar a liberdade de expressão e de informação;
  + tiver de conservar os dados pessoais para cumprir uma obrigação jurídica;
  + existirem outros motivos de interesse público na conservação dos dados pessoais, como finalidades de saúde pública ou de investigação científica e histórica;
  + tiver de conservar os dados pessoais para a declaração de um direito num processo judicial.

**direito à retificação e direito de se opor**

* Se um indivíduo considerar que os seus dados pessoais estão incorretos, incompletos ou inexatos, o indivíduo tem o direito a que estes sejam retificados ou completados sem demora injustificada.
* Um indivíduo também pode opor-se, a qualquer momento, ao tratamento dos seus dados pessoais para uma utilização específica se a sua empresa efetuar o respetivo tratamento com base no seu interesse legítimo ou para o exercício de uma função de interesse público. A menos que a empresa tenha um interesse legítimo que se sobreponha ao interesse do indivíduo, tem de interromper o tratamento dos dados pessoais. Do mesmo modo, um indivíduo pode pedir a limitação do tratamento dos seus dados pessoais enquanto se determina se o interesse legítimo da empresa se sobrepõe ou não ao interesse do indivíduo. No entanto, em caso de comercialização direta, a empresa é sempre obrigada a interromper o tratamento dos dados pessoais a pedido do indivíduo

**nomear um encarregado da proteção de dados (EPD)**

* Um EPD é responsável por controlar a conformidade da sua empresa com o RGPD. Uma das principais funções do EPD consiste em informar e aconselhar os trabalhadores que efetuam o tratamento de dados pessoais propriamente dito sobre as suas obrigações

**proteção de dados desde a conceção e por defeito**

* A proteção de dados desde a conceção ajuda a garantir que uma empresa tem em conta a proteção de dados nas fases iniciais do planeamento de uma nova forma de tratamento de dados pessoais.
* A proteção de dados desde a conceção ajuda a garantir que uma empresa tem em conta a proteção de dados nas fases iniciais do planeamento de uma nova forma de tratamento de dados pessoais.

**assegurar a devida notificação em caso de violação de dados**

* Uma violação de dados ocorre quando os dados pessoais pelos quais é responsável são divulgados, quer acidental quer ilegalmente, a destinatários não autorizados ou são alterados ou indisponibilizados temporariamente
* A empresa pode também ter de informar todos os indivíduos afetados pela violação de dados, dependendo de se esta representa ou não um risco elevado para os indivíduos afetados.

O incumprimento do RGPD pode dar origem a coimas significativas — até 20 milhões de euros ou 4% do volume de negócios global de uma empresa, para determinadas violações. A APD pode impor medidas corretivas adicionais, como ordenar a cessação do tratamento de dados pessoais. Também deve ter em conta os danos em termos de reputação que poderão ser causados pelo incumprimento.

Claramente, os custos do incumprimento do RGPD são muito superiores do que qualquer investimento realizado para o cumprir.

A sua autoridade de proteção de dados local efetua o controlo do cumprimento; o seu trabalho é coordenado

## Descreva por suas palavras quais as entidades ao qual nao se aplicam as medidas de direitos, adaptação e prova do RGPD?

RESPOSTA:

A segurança do estado, nomeadamente a parte federal, tribunais

A defesa, nomeadamente o exército

A seguranca publica - policia

**OUTRO**

A sua empresa é uma prestadora de serviços e está sediada fora da UE. Presta serviços a clientes fora da UE. Os clientes podem utilizar os seus serviços quando viajam para outros países, incluindo dentro da UE. Desde que a sua empresa não dirija especificamente os seus serviços a pessoas na UE, não está sujeita às regras do RGPD.

## Privacy by design & Privacy by default

**Alternativa 1 - Mais Pobre em conteúdo**

O termo significa “desde a conceção”. Privacy by design poderia ser traduzido por “proteção pensada por defeito e desde a criação de qualquer projeto que implique um tratamento de dados”. Para além do campo semântico, o que conta é adaptar o quadro em que os dados são recolhidos e utilizados. De facto, a proteção de dados pessoais não é uma filosofia ou um simples valor. É um princípio arvorado em regra. Cada empresa deve provar que integra a questão da proteção e da segurança dos dados desde a implementação do tratamento. É, por conseguinte, uma restrição que permite regular melhor o fluxo. Possui uma nova aplicação móvel? Uma nova estratégia de emailing? Conteúdos para partilhar com a sua comunidade? A questão da gestão dos dados deve ser considerada da mesma forma que o webdesign, a experiência do utilizador ou os seus objetivos comerciais.

**Alternativa 2**

O RGPD introduz dois novos princípios: o da proteção de dados desde a conceção e o da proteção de dados

por defeito.

**(Privacy by design)**

**A proteção de dados desde a conceção** ajuda a garantir que uma empresa tem em conta a proteção de dados nas fases iniciais do planeamento de uma nova forma de tratamento de dados pessoais. De acordo

com este princípio, um responsável pelo tratamento deve tomar todas as medidas técnicas e organizativas

necessárias para aplicar os princípios da proteção e dados e para proteger os direitos dos indivíduos.

Estas medidas podem incluir, por exemplo, o recurso à pseudonimização.

**A proteção de dados desde a conceção** minimiza os riscos para a privacidade e reforça a confiança. Ao privilegiar a proteção de dados aquando do desenvolvimento de novos bens ou serviços, poderá evitar possíveis problemas relacionados com a proteção de dados logo numa fase inicial. Além disso, esta prática ajuda a sensibilizar todos os departamentos e níveis de uma empresa para a proteção de dados.

**(Privacy by default)**

**A proteção de dados por defeito** implica a garantia, por parte da sua empresa, de que a configuração mais favorável à privacidade é sempre a configuração predefinida. Por exemplo, se forem possíveis duas configurações de privacidade e uma delas impedir o acesso de terceiros aos dados pessoais, esta deve ser utilizada como a configuração por defeito.

## As responsabilidades dos responsáveis pelo tratamento ou subcontratados não estabelecidos na união europeia(ex: como os dados da google saem cá para fora)?

No mundo globalizado de hoje, existem grandes quantidades de transferências transfronteiriças de dados pessoais, que, por vezes, são armazenados em servidores situados em vários países diferentes.

A proteção concedida pelo Regulamento Geral sobre a Proteção de Dados (RGPD) viaja com os dados, o que significa que as regras que protegem os dados pessoais continuam a aplicar-se independentemente da localização dos dados. Tal aplica-se também quando os dados são transferidos para um país que não seja membro da UE («país terceiro»).

O RGPD proporciona diferentes instrumentos para enquadrar as transferências de dados de um país da UE para um país terceiro:

* em certos casos, pode declarar-se que um país terceiro oferece um nível adequado de proteção através de uma decisão da Comissão Europeia («decisão de adequação»), o que significa que é possível transferir dados para uma empresa situada no país terceiro sem que o exportador dos dados tenha de apresentar garantias suplementares e sem que esteja sujeito a condições adicionais. Por outras palavras, as transferências para um país terceiro «adequado» serão semelhantes a uma transmissão de dados no interior da UE.
* na falta de uma decisão de adequação, a transferência pode ser efetuada mediante a apresentação de garantias adequadas e na condição de as pessoas gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes. Estas garantias adequadas incluem, nomeadamente, as seguintes:
* no caso de um grupo de empresas ou de grupos de empresas envolvidos numa atividade económica conjunta, as empresas podem transferir dados pessoais com base nas chamadas regras vinculativas aplicáveis às empresas;
* disposições contratuais com o destinatário dos dados pessoais, utilizando, por exemplo, as cláusulas-tipo de proteção de dados adotadas pela Comissão Europeia;
* adesão a um código de conduta ou um procedimento de certificação, acompanhado de compromissos vinculativos e com força executiva assumidos pelos destinatários no sentido de aplicarem as garantias adequadas para proteger os dados transferidos.
* por último, se estiver prevista uma transferência de dados pessoais para um país terceiro que não esteja sujeito a uma decisão de adequação e na ausência de garantias adequadas, a transferência pode ser efetuada com base num conjunto de derrogações aplicáveis em situações específicas, por exemplo se uma pessoa tiver consentido expressamente na transferência proposta após ter recebido todas as informações necessárias sobre os riscos associados à mesma.

## **Exemplo**

Uma empresa francesa tenciona expandir os seus serviços à América do Sul, nomeadamente à Argentina, ao Uruguai e ao Brasil. O primeiro passo seria o de verificar se tais países terceiros são objeto de uma decisão de adequação. Neste caso, tanto a Argentina como o Uruguai foram declarados adequados. A empresa poderia transferir dados pessoais para estes dois países não pertencentes à UE sem garantias adicionais, ao passo que as transferências para o Brasil, que não é objeto de uma decisão de adequação, terão de ser efetuadas mediante a apresentação de

## Quais são as actividades do responsável pelo tratamento de dados?

Cada responsável pelo tratamento ou subcontratante que efetue tratamento de dados, de acordo com o Artigo 30º torna-se obrigado a manter e conservar um registo de todas as atividades de tratamento que efetuem sob a sua responsabilidade.

É aconselhável descrever um conjunto específico de informações devidamente definido que identifique cada tratamento de dados, designadamente:

* Tipo de dados recolhidos;
* – Finalidades de cada tratamento;
* – Categorias de dados tratadas;
* – Transmissão de dados para países terceiros;
* – Período de conservação dos dados;
* – Onde os dados estão armazenados;
* – Contactos do responsável pelo tratamento;

Pode-se assim deferir, por exemplo, a tabela com seguinte informação:

É igualmente exigido, a cada subcontratante, a conservação de um registo com todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento.  
  
No caso do tratamento de dados pessoais a crianças que tenham menos de 16 anos, o tratamento só é lícito desde que o consentimento seja dado ou autorizado pelos titulares parentais da criança, referido no Artigo 8º, n.1º.  
  
De forma a ser realizada a verificação de conformidade, a Autoridade de Controlo pode solicitar, a qualquer momento, ao responsável pelo tratamento a disponibilização dos registos das Atividades de Tratamento

## Descreva a finalidade, a pertinência e a obrigatoriedade da avaliação de impacto(AIPD)?

A Avaliação do Impacto de Privacidade, em inglês PIA (Privacy Impact Assessement), deve decorrer especialmente nos casos em que o tratamento dos dados pessoais é efetuado através do uso de novas

tecnologias. Essa avaliação deverá considerar a natureza dos dados, o âmbito, o contexto e a finalidade dos mesmos.

Sempre que o tratamento efetuado apresente suscetibilidade de implicar um elevado risco para os direitos e liberdades dos titulares, o responsável pelo tratamento deverá fazer uma avaliação do impacto das operações previstas na proteção dos dados pessoais, antes de iniciar o tratamento.

**É obrigatório** realizar uma AIPD sempre que o tratamento pretendido resulte num elevado risco para os direitos e as liberdades dos indivíduos. Este pode ser o caso, por exemplo, da utilização de novas tecnologias.

A **AIPD tem por objetivo** identificar potenciais riscos para os direitos e as liberdades dos indivíduos antes do início do tratamento de dados pessoais e antes de o risco se concretizar. Ao atenuar o risco antecipadamente, é possível evitar danos e minimizar os riscos.

Se as medidas previstas na AIPD não eliminarem todos os riscos elevados identificados, a APD deve ser consultada antes do início do tratamento de dados pretendido.

A realização de um PIA (Privacy Impact Assessement) é obrigatória nas seguintes situações:

**ESCOLHER UMA ALTERNATIVA**

**ALTERNATIVA 1** (MAIS COMPLETO)

1. Quando é feita uma avaliação de aspetos pessoais com base no tratamento automatizado de dados, incluindo definição de perfis que produzem efeitos jurídicos relativamente à pessoa singular.
2. Quando existe tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais ou infrações.
3. Quando é realizado um controlo sistemático de zonas acessíveis ao público em grande escala.

**ALTERNATIVA 2** (MAIS RESUMIDO)

1. são utilizados mecanismos de tratamento automatizado e definição de perfis para avaliar indivíduos de forma sistemática e completa;
2. um espaço acessível ao público é controlado de forma sistemática e em grande escala (por exemplo, CCTV);
3. é efetuado o tratamento de dados sensíveis em grande escala (por exemplo, dados de saúde).

## Quais sao as funcoes do DPO?

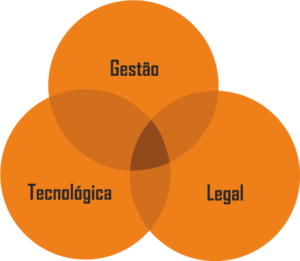
A existência de uma função chamada Encarregado de Protecção de Dados (EPD) ou *Data Protection Officer (DPO)* não é obrigatória, mas é recomendada em todas as organizações que tratem dados pessoais ou sensíveis.

Tem o regime previsto nos Artigos 37º, 38º e 39º do RGPD, ficando sujeito ao dever e sigilo ou confidencialidade bem como ao dever de incompatibilidade, não podendo exercer quaisquer funções e atribuições que resultem de um conflito de interesses para o exercício das funções.

A designação do DPO deve ser realizada em função das competências profissionais em especial dos conhecimentos avançados de proteção de dados e que seja capaz de cumprir as tarefas atribuídas no Artigo 39º, relacionadas com a segurança e proteção de dados, por exemplo deve ter as seguintes funções:

* – Sensibilização e informar todos os que tratem dados pessoais;
* – Assegurar o comprimento das políticas de privacidade e proteção de dados;
* – Controlar e regular a conformidade do RGPD;
* – Recolher informação para identificar atividades de tratamento;
* – Controlar e acompanhar a produção do AIPD – Avaliação de Impacto sobre Proteção de Dados;
* – Promover as abordagens de Privacidade por Desenho e por Padrão;
* – Realizar a avaliação na exposição aos riscos de violações de privacidade e mitigados com ações de melhoramento;
* – Recolher informação para identificar atividades de tratamento;
* – Manter atualizado os registos das atividade de tratamento de dados;
* – Controlar o cumprimento de contratos escritos subcontratante;
* – Promover formações de boas práticas para a proteção de dados;
* – Ser o ponto de contacto com os titulares de dados de forma a esclarecer questões relacionadas com o tratamento dos dados;
* – Ser o ponto de contacto com as autoridades de controlo;

Percebe-se que idealmente deveria ser alguém capaz de conciliar conhecimentos de, pelo menos, as seguintes áreas: tecnológica, gestão, e legal.



Embora seja uma dúvida nos termos do RGPD, é claro que uma das competências do DPO está relacionada com gestão, infraestruturas de TI e coordenação de auditorias SI, e por isso uma experiência nestas áreas é uma mais valia para qualquer profissional desempenhar as suas funções com agilidade e competência.

Todas as questões relacionadas com a segurança e proteção de dados, o DPO deve exercer com a máxima independência e ser sempre envolvido de forma adequada a tempo útil, apoiado por uma equipa multidisciplinar que reúna competências nas mais diversas áreas (financeira, recursos humanos, tecnológica, marketing, arquivo e entre outras) fornecendo os recursos necessários para o desempenho das funções tratadas pelo responsável pelo tratamento e subcontratantes.

O DPO assume, assim, a responsabilidade na aplicação da estratégia para proteção dos dados e conformidade do RGPD. Todo o descuido em eventuais não conformidades e incidentes ou violações serão imputadas ao responsável pelo tratamento, em última instância à administração.

Trata-se de uma função bastante exigente, mas aliciante e certamente será um perfil muito procurado nos próximos tempos.

## O que e considerado dados em grande escala?

O RGPD exige a designação obrigatória de um EPD sempre que o tratamento de dados pessoais seja realizado em grande escala, mas não define em que consiste o tratamento de grande escala.

Apenas são dadas algumas linhas de orientação nos considerandos iniciais do regulamento, embora se refiram às avaliações do impacto sobre a protecção de dados.

Assim, o EPD é obrigatório quando se trate de tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, que possam afectar um número considerável de titulares de dados e sejam susceptíveis de implicar um elevado risco.

Não deve ser considerado de grande escala quando diga respeito aos dados pessoais de clientes de advogados ou pacientes de médicos, profissionais de cuidados de saúde.

Contudo, entre dois extremos – como o tratamento de dados por um médico e o tratamento de dados de um país inteiro ou à escala da Europa - existe uma zona cinzenta que precisa ser definida, na qual não é possível quantificar um número preciso quanto ao volume de dados tratados ou ao número de pessoas em causa que seria aplicável em todas as situações.

Existe tratamento de grande escala, por exemplo, no tratamento de dados:

* De dados de viagem das pessoas que usam o sistema de transportes públicos de uma cidade (através dos passes de viagem por exemplo);
* Em tempo real de dados de geolocalização de clientes de uma cadeia de restauração rápida internacional para fins estatísticos por parte de um subcontratante especializado na prestação desses serviços;
* De clientes no exercício normal das actividades de uma companhia de seguros ou de um banco;
* Para fins de publicidade comportamental por um motor de busca;
* De dados por operadoras telefónicas ou fornecedores de serviços de internet (conteúdo, tráfego, localização);
* De doentes no exercício normal das actividades de um hospital.

Não constituem tratamento de grande escala, nomeadamente:

* o tratamento de dados de doentes pacientes por um médico;
* o tratamento de dados pessoais relacionados com condenações penais e infrações por um advogado.

Portanto, para determinar se um tratamento é efectuado em grande escala, a recomendação do Grupo de Trabalho encarregue de dar uniformização à aplicação do RGPD é que se tome em consideração os seguintes factores:

* o número de titulares de dados afectados (número concreto ou percentagem da população em causa);
* o volume de dados e/ou o alcance dos diferentes elementos de dados objecto de tratamento;
* a duração, ou permanência, da actividade de tratamento de dados;
* o âmbito geográfico da actividade de tratamento.

## CASOS DE OBRIGAÇÃO OU NÃO DE TER EPD

Certos responsáveis pelo tratamento de dados e subcontratantes devem obrigatoriamente designar um EPD, como é o caso de todas as autoridades e organismos públicos (independentemente do tipo de dados que tratam) e de outras organizações cuja actividade principal consista no controlo de pessoas de forma sistemática e em grande escala, ou que tratam de categorias especiais de dados pessoais em larga escala.

Mesmo quando o RGPD não exige especificamente a nomeação de um EPD, as organizações podem, nalguns casos, considerar conveniente designar um a título voluntário.

Os EPD não são pessoalmente responsáveis em caso de incumprimento do RGPD. É ao responsável pelo tratamento ou ao subcontratante que co

mpete assegurar e comprovar que o tratamento é realizado em conformidade com as suas regras.

O conceito de EPD não é novo; já estava previsto na Directiva de 1995 que é agora substituída pelo RGPD mas esta não obrigava qualquer organização a nomear um EPD.

Contudo, o seu papel mudou e é considerado um pilar da responsabilidade em matéria de tratamento de dados, nomeadamente viabilizando avaliações de impacto sobre a protecção de dados e efectuando ou viabilizando auditorias.

Além disso os EPD servem de intermediários entre as partes interessadas - as autoridades de controlo, os titulares de dados e as unidades empresariais dentro de uma organização.

Acontece que mesmo que o responsável pelo tratamento preencha os critérios de designação obrigatória, o seu subcontratante não tem necessariamente de nomear um EPD, embora isso possa constituir uma boa prática.

Será o caso de uma pequena empresa familiar de distribuição de eletrodomésticos numa localidade que usa os serviços de um subcontratante que lhe presta serviços analíticos e de assistência no site, com publicidade e marketing direcionados. As actividades da empresa familiar e os seus clientes não são um tratamento de dados «em grande escala», atendendo ao número reduzido de clientes e ao âmbito relativamente limitado das actividades.

No entanto, globalmente, as actividades do subcontratante, com muitos clientes, a exemplo desta pequena empresa, acarretam um tratamento de grande escala. Em consequência, o subcontratante terá de designar um EPD. A empresa familiar não é obrigada a designar individualmente um EPD.

Uma empresa de média dimensão que, por exemplo fabrique ladrilhos e subcontrate os seus serviços de medicina do trabalho a um subcontratante externo que tenha um grande número de clientes semelhantes não está necessariamente sujeita à obrigação de designar um EPD, mas o subcontratante estará desde que o tratamento seja efetuado em grande escala.

Referências:

[Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27.04.2016](https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT)

[Lei n.º 67/98 de 26 de Outubro, artigo 37.º, n.º 1, alíneas b) e c)](https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm)

[Proposta de Lei n.º 120/XIII, de 26.03.2018 (GOV)](http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true)

## Categorias Especiais de Dados Pessoais

﻿O tratamento de categorias especiais de dados pessoais é proibido, salvo nos casos apresentados no n.º 2 do artigo 9.º do RGPD. Todos estes dados têm restrições adicionais de tratamento pelo que se recomenda a leitura atenta das secções respetivas do RGPD.

**São categorias especiais de dados pessoais:**

* a origem racial ou étnica;
* as opiniões políticas;
* as convicções religiosas;
* as convicções filosóficas;
* a filiação sindical;
* os dados genéticos;
* os dados biométricos para identificar uma pessoa de forma inequívoca;
* os dados relativos à saúde;
* os dados relativos à vida sexual ou orientação sexual de uma pessoa.

**﻿Dados genéticos são definidos como**: "Os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa" (RGPD, Artº 4, nº 13).

**Dados biométricos são definidos como** "Dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos" (RGPD, Art. 4º, nº 14).

**Dados relativos à saúde são definidos como** "Dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde"(RGPD, Art. 4º, nº 15).

## Transferência de dados pessoais para fora da UE

O RGPD aplica-se no Espaço Económico Europeu (EEE), que inclui todos os países da UE e ainda a Islândia, o Listenstaine e a Noruega. Quando os dados pessoais são transferidos para fora do território do EEE, as proteções concedidas pelo RGPD viajam com esses dados. Isto significa que, para exportarem dados para o estrangeiro, as empresas têm de assegurar a aplicação de determinadas garantias.

O RGPD oferece um conjunto diversificado de mecanismos para transferir dados para países terceiros. De acordo com o RGPD, essas transferências são permitidas quando:

1. as proteções do país são consideradas adequadas pela UE; ou
2. a sua empresa, por exemplo, toma as medidas necessárias para conceder garantias adequadas, nomeadamente incluindo cláusulas específicas no contrato celebrado com o importador não europeu dos dados pessoais; ou
3. a sua empresa, por exemplo, baseia-se em fundamentos específicos para a transferência (as chamadas «derrogações»), como o consentimento do indivíduo.

## Quando e que uma empresa esta a cumprir o RGPD

No que diz respeito ao tratamento de dados pessoais, o RGPD passa a bola para o seu lado. O primeiro

passo consiste em efetuar um levantamento das suas atividades atuais de tratamento de dados e reavaliar os

seus processos empresariais internos. Deve, em especial:

* identificar que dados detém e para que finalidades e com que base jurídica os detém;
* avaliar todos os contratos em vigor, em especial entre responsáveis pelo tratamento e subcontratantes;
* avaliar todas as vias disponíveis de transferência de dados;
* analisar a governação global da sua empresa (ou seja, que medidas informáticas e organizativas possui), incluindo se tem de nomear ou se pretende nomear um encarregado da proteção de dados.

Um elemento essencial deste processo consiste em garantir que o nível mais elevado de gestão da sua empresa participa nestas revisões, contribui para as mesmas e é regularmente atualizado e consultado sobre alterações à política de dados.