GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS

17/PT

WP 253

Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679

Adotadas em 3 de outubro de 2017

Este grupo de trabalho foi criado nos termos do artigo 29.º da Diretiva 95/46/CE. Trata-se de um organismo consultivo independente europeu em matéria de proteção de dados e de privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

O secretariado é assegurado pela Direção C (Direitos Fundamentais e Cidadania da União) da Direção-Geral da Justiça da Comissão Europeia, B-1049, Bruxelas, Bélgica, Gabinete n.º MO-59 03/075.

Sítio: http://ec.europa.eu/justice/data-protection/index_en.htm

O GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO

TRATAMENTO DE DADOS PESSOAIS

criado pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º,

Tendo em conta o seu regulamento interno,

ADOTOU AS PRESENTES DIRETRIZES:

Índice:

I. Introdução 4
II. Princípios 5
III. Critérios de avaliação do artigo 83.º, n.º 2 9
IV. Conclusão 18

I. Introdução

A UE concluiu uma profunda reforma do regulamento da proteção de dados na Europa. A reforma assenta em vários pilares (principais componentes): normas coerentes, procedimentos simplificados, ações coordenadas, participação dos utilizadores, informações mais eficazes e poderes coercivos reforçados.

Os responsáveis pelo tratamento e os seus subcontratantes têm responsabilidades acrescidas para garantir a proteção eficaz dos dados pessoais. As autoridades de controlo têm competência para assegurar que os princípios do Regulamento Geral da Proteção de Dados (a seguir designado «regulamento»), assim como os direitos das pessoas em questão, são respeitados em conformidade com a letra e o espírito do regulamento.

A coerente aplicação das normas de proteção de dados é crucial para um regime de proteção de dados harmonizado. As coimas constituem um elemento central do novo regime de execução introduzido pelo regulamento, representando um forte elemento do conjunto de ferramentas de execução das autoridades de controlo, a par das outras medidas previstas no artigo 58.º.

O presente documento destina-se a ser utilizado pelas autoridades de controlo para garantir uma melhor aplicação e execução do regulamento e expõe o seu entendimento comum do disposto no artigo 83.º do regulamento, bem como da articulação deste com os artigos 58.º e 70.º e com os considerandos que lhes estão associados.

Nomeadamente, de acordo com o artigo 70.º, n.º 1, alínea e), o Comité Europeu para a Proteção de Dados (CEPD) está habilitado a emitir diretrizes, recomendações e boas práticas, a fim de incentivar a aplicação coerente do regulamento, sendo que o artigo 70.º, n.º 1, alínea k), se refere especificamente à emissão de diretrizes em matéria de fixação de coimas.

Estas diretrizes não são exaustivas, nem tão-pouco fornecem explicações acerca das diferenças entre os sistemas de direito administrativo, civil ou penal ao impor coimas no geral.

Tendo em vista uma abordagem coerente no atinente à imposição de coimas, que reflita adequadamente todos os princípios contidos nestas diretrizes, o CEPD chegou a acordo quanto a um entendimento comum dos critérios de avaliação constantes do artigo 83.º, n.º 2, do regulamento e, por conseguinte, o CEPD e as autoridades de controlo concordam na utilização das presentes diretrizes enquanto abordagem comum.

II. Princípios

Quando for determinada uma infração ao regulamento com base na avaliação dos factos do caso, a autoridade de controlo competente deve identificar a(s) medida(s) corretiva(s) mais adequada(s) para sanar a infração. O disposto no artigo 58.º, n.º 2, alíneas b) a j)[1], indica quais as ferramentas que as autoridades de controlo podem empregar a fim de corrigir uma situação de incumprimento por parte de um responsável pelo tratamento de dados ou subcontratante. Ao fazerem uso desses poderes, as autoridades de controlo devem respeitar os seguintes princípios:

---

1. As infrações ao regulamento devem conduzir à imposição de «sanções equivalentes».

O conceito de «equivalência» é fulcral para determinar o âmbito das obrigações das autoridades de controlo, a fim de assegurar a coerência na utilização que estas fazem dos poderes de correção nos termos do artigo 58.º, n.º 2, em geral, e na aplicação de coimas, em particular[2].

«A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, ***o nível de proteção [...] deverá ser equivalente*** *em todos os Estados-Membros.»* (considerando 10). O considerando 11 discorre sobre o facto de um nível equivalente de proteção dos dados pessoais na União exigir, entre outras coisas, «*poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros*». Além disso, a aplicação de sanções equivalentes em todos os Estados-Membros, bem como uma cooperação eficaz entre as autoridades de controlo dos diferentes Estados-Membros, são vistas como uma forma de «*evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno*», de acordo com o considerando 13 do regulamento.

O regulamento estabelece uma base mais sólida do que a Diretiva 95/46/CE para um maior nível de coerência, uma vez que o regulamento é diretamente aplicável nos Estados-Membros. Embora as autoridades de controlo ajam com *«total independência»* (artigo 52.º) relativamente aos governos nacionais, responsáveis pelo tratamento ou subcontratantes, estão obrigadas a cooperar *«tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento»* [artigo 57.º, n.º 1, alínea g)].

Mais do que a Diretiva 95/46/CE, o regulamento insta a uma maior coerência na imposição de sanções. Nos casos transnacionais, a coerência é principalmente assegurada através do mecanismo de cooperação (balcão único) e, em certa medida, através do procedimento de controlo da coerência previsto pelo novo regulamento.

Nos casos nacionais abrangidos pelo regulamento, as autoridades de controlo aplicarão estas diretrizes num espírito de cooperação, em conformidade com o artigo 57.º, n.º 1, alínea g), e com o artigo 63.º, com vista a assegurar a coerência da aplicação e da execução do regulamento. Embora mantenham a

[1] O artigo 58.º, n.º 2, estipula que podem ser feitas advertências quando *«as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento»*. Por outras palavras, no caso abrangido pela disposição acima, a infração ao regulamento ainda não teve lugar.

[2] Mesmo nos casos em que os sistemas jurídicos de alguns países da UE não permitem a imposição de coimas conforme prevista no regulamento, a aplicação das normas desses Estados-Membros tem de ter um efeito equivalente às coimas impostas pelas autoridades de controlo (considerando 151). Os tribunais encontram-se vinculados pelo regulamento, mas não pelas presentes diretrizes do CEPD.

autonomia na escolha das medidas corretivas apresentadas no artigo 58.º, n.º 2, as autoridades de controlo devem evitar escolher medidas corretivas diferentes para casos semelhantes.

O mesmo princípio se aplica às medidas que forem impostas sob a forma de coimas.

2. Como todas as medidas corretivas escolhidas pelas autoridades de controlo, as coimas devem ser «efetivas, proporcionadas e dissuasivas».

Como todas as medidas corretivas em geral, as coimas devem dar resposta adequada à natureza, gravidade e consequências da violação, devendo as autoridades de controlo avaliar todos os factos do caso de forma coerente e objetivamente justificada. A avaliação daquilo que é efetivo, proporcionado e dissuasivo em cada caso individual terá de refletir também o objetivo da medida corretiva selecionada, quer se trate de restaurar o cumprimento das normas, quer de punir um comportamento ilícito (ou ambos).

As autoridades de controlo devem escolher uma medida corretiva *«efetiva, proporcionada e dissuasiva»* (artigo 83.º, n.º 1), tanto em casos nacionais (artigo 55.º) como em casos que impliquem o tratamento transnacional de dados pessoais (na aceção do artigo 4.º, n.º 23).

Estas diretrizes reconhecem que a legislação nacional pode impor requisitos adicionais para o procedimento de execução a observar pelas autoridades de controlo. Tal pode nomeadamente incluir notificações de endereço, formulários, prazos para apresentação de alegações, recursos, execução e pagamento[3].

Contudo, tais requisitos não devem impedir, na prática, a consecução da efetividade, da proporcionalidade ou do caráter dissuasivo.

Uma determinação mais precisa da efetividade, da proporcionalidade ou do caráter dissuasivo será efetuada com base na prática emergente no seio das autoridades de controlo (em matéria de proteção de dados, mas também de lições retiradas de outros domínios regulados), assim como na jurisprudência resultante da interpretação desses princípios.

A fim de impor coimas efetivas, proporcionadas e dissuasivas, a autoridade de controlo deve utilizar a definição do conceito de empresa prevista pelo TJUE para efeitos da aplicação dos artigos 101.º e 102.º do TFUE, nomeadamente o facto de por empresa **se entender** uma unidade económica, que pode ser constituída pela empresa-mãe e por todas as eventuais filiais. Em conformidade com o direito e a jurisprudência da UE[4], por empresa deve entender-se uma unidade económica que exerça atividades comerciais/económicas, independentemente da pessoa coletiva em causa (considerando 150).

[3] A título de exemplo, o quadro constitucional e as propostas de legislação de proteção de dados da Irlanda preveem que seja tomada uma decisão formal quanto à própria infração, que é comunicada às partes, antes de se proceder à avaliação da severidade da sanção ou sanções. A decisão quanto à própria infração não pode ser revista durante a avaliação da severidade da sanção ou sanções.

[4] A definição constante da jurisprudência do Tribunal de Justiça é a seguinte: *«O conceito de empresa abrange qualquer entidade que exerça uma atividade económica, independentemente do seu estatuto jurídico e modo de funcionamento»* (Processo Höfner e Elser, n.º 21, ECLI:EU:1991:161). O conceito de empresa *«deve ser entendido como designando uma unidade económica [...] mesmo que, do ponto de vista jurídico, essa unidade económica seja constituída por várias pessoas singulares ou coletivas»* [Processo *Confederación Española de Empresarios de Estaciones de Servicio* (n.º 40, ECLI:EU:C:2006:784)].

3. A autoridade de controlo competente fará uma avaliação «em cada caso individual».

As coimas podem ser impostas em resposta a um amplo leque de infrações. O artigo 83.º do regulamento prevê uma abordagem harmonizada das violações de obrigações expressamente enumeradas nos n.os 4 a 6. O direito de um Estado-Membro pode tornar a aplicação do artigo 83.º extensiva a autoridades públicas e a organismos estabelecidos no território desse Estado-Membro. Além disso, o direito de um Estado-Membro pode permitir ou até mandatar a imposição de uma coima em razão da infração a outras disposições para além das referidas no artigo 83.º, n.os 4 a 6.

O regulamento exige a avaliação de cada caso individualmente[5]. O artigo 83.º, n.º 2, é o ponto de partida para esta avaliação individual. Esse número refere que *«[a]o decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte [...]»*. Em conformidade com o que precede, e à luz também do considerando 148[6], a autoridade de controlo é responsável pela escolha da(s) medida(s) mais adequada(s). Nos casos mencionados no artigo 83.º, n.os 4 a 6, esta escolha **tem** de ter em conta todas as medidas corretivas, o que implica considerar a imposição da coima adequada, quer conjugada com uma medida corretiva nos termos do artigo 58.º, n.º 2, quer autonomamente.

As coimas são uma ferramenta importante, que deve ser utilizada pelas autoridades de controlo em circunstâncias adequadas. As autoridades de controlo são incentivadas a adotar uma abordagem ponderada e equilibrada no que se refere à utilização de medidas corretivas, a fim de assegurar uma resposta à infração que seja simultaneamente efetiva, dissuasiva e proporcionada. O objetivo consiste em não qualificar as coimas como último recurso e em não evitar a sua aplicação, embora, por outro lado, não se deva recorrer às coimas de uma forma que prejudique a sua efetividade enquanto ferramenta.

[5] Para além da aplicação dos critérios constantes do artigo 83.º, existem outras disposições que reforçam a base desta abordagem, nomeadamente:

- Considerando 141 – *«[a] investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico.»*
- Considerando 129 – *«[o]s poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com o presente regulamento, tendo em conta as circunstâncias de cada caso concreto [...].»*
- Artigo 57.º, n.º 1, alínea f) – *«tratar as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.º, e investigar, na medida do necessário, o conteúdo da reclamação [...].»*

[6] *«A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo nos termos do presente regulamento. Em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima. Importa, porém, ter em devida conta a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções, incluindo coimas, deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo.»*

O CEPD, quando competente em conformidade com o artigo 65.º do regulamento, emitirá uma decisão vinculativa relativa a litígios entre autoridades no que se refere, em especial, à determinação da existência de violação. Nos casos em que a objeção pertinente e fundamentada suscite a questão da conformidade da medida corretiva com o RGPD, a decisão do CEPD versará também o modo como os princípios da efetividade, proporcionalidade e dissuasão são observados na coima proposta no projeto de decisão da autoridade de controlo competente. Numa fase posterior, serão apresentadas separadamente orientações do CEPD relativas à aplicação do artigo 65.º do regulamento, para maior detalhe sobre o tipo de decisão a tomar pelo CEPD.

4. A abordagem harmonizada das coimas no domínio da proteção de dados exige a participação ativa e o intercâmbio de informações entre autoridades de controlo

As presentes diretrizes reconhecem que as competências em matéria de coimas representam, para algumas autoridades de controlo nacionais, uma novidade no domínio da proteção de dados, suscitando várias questões em termos de recursos, organização e procedimento. Nomeadamente, as decisões mediante as quais as autoridades de controlo exercem as competências que lhes forem conferidas em matéria de imposição de coimas, serão passíveis de recurso junto dos tribunais nacionais.

As autoridades de controlo devem cooperar entre si e, se for caso disso, com a Comissão Europeia, através dos mecanismos de cooperação estabelecidos no regulamento, a fim de apoiar intercâmbios formais e informais de informações, designadamente através de seminários regulares. Tal cooperação deve incidir na sua experiência e prática na aplicação das competências em matéria de coimas, a fim de, em última instância, adquirirem maior coerência.

Para além de suscitar jurisprudência relativa à utilização dessas competências, o intercâmbio proativo de informações pode levar a um reexame dos princípios ou de pormenores específicos das presentes diretrizes.

III. Critérios de avaliação do artigo 83.º, n.º 2

O artigo 83.º, n.º 2, prevê uma lista de critérios que as autoridades de controlo devem utilizar ao avaliar da pertinência da imposição de uma coima e determinar o montante da mesma. Não é recomendada uma avaliação repetida dos mesmos critérios, mas antes uma avaliação que tenha em conta todas as circunstâncias de cada caso, nos termos do artigo 83.º[7].

As conclusões alcançadas na primeira fase da avaliação podem ser utilizadas na segunda, relativa ao montante da coima, tornando desnecessária uma dupla avaliação com base nos mesmos critérios.

Esta secção fornece às autoridades de controlo orientações para interpretar os factos individuais do caso à luz dos critérios do artigo 83.º, n.º 2.

a) A natureza, a gravidade e a duração da infração

Quase todas as obrigações dos responsáveis pelo tratamento e dos subcontratantes nos termos do regulamento se encontram categorizadas de acordo com a sua **natureza** no artigo 83.º, n.os 4 a 6. Ao estabelecer dois montantes máximos distintos para as coimas (10/20 milhões de EUR), o regulamento indica desde logo que existem disposições cuja violação pode ser mais grave do que a de outras. Contudo, a autoridade de controlo competente, mediante avaliação dos factos do caso à luz dos critérios gerais enunciados no artigo 83.º, n.º 2, pode decidir que num caso específico existe uma necessidade acrescida ou reduzida de reagir por meio de uma medida corretiva sob a forma de coima. Se a coima for considerada a medida ou uma das medidas corretivas adequadas, será aplicado o sistema de limiares do regulamento (artigo 83.º, n.os 4 a 6), a fim de identificar a coima máxima que pode ser imposta de acordo com a natureza da infração em causa.

O considerando 148 introduz o conceito de «infrações menores». Tais infrações podem constituir violações de uma ou várias normas enunciadas no artigo 83.º, n.os 4 ou 5, do regulamento. A avaliação dos critérios constantes do artigo 83.º, n.º 2, pode, contudo, levar a autoridade de controlo a entender que, nas circunstâncias concretas do caso, por exemplo, a violação não constitui um risco significativo para os direitos dos titulares dos dados em causa, nem tão-pouco afeta a essência da obrigação pertinente. Nesses casos, a coima pode (embora nem sempre) ser substituída por uma repreensão.

O considerando 148 não estabelece a obrigação de a autoridade de controlo substituir invariavelmente uma coima por uma repreensão em caso de infração menor (*«pode ser feita uma repreensão em vez de ser aplicada a coima»*), mas sim uma possibilidade existente, na sequência da avaliação concreta de todas as circunstâncias do caso.

O considerando 148 prevê essa mesma possibilidade de substituir a coima por uma repreensão nos casos em que o responsável pelo tratamento seja uma pessoa singular relativamente à qual o montante da coima constitua um ónus desproporcionado. Como ponto de partida, a autoridade de controlo tem de avaliar se, dadas as circunstâncias do caso em apreço, é necessário impor uma coima. Se decidir fazê-lo, terá ainda de avaliar se a coima a aplicar constitui um ónus desproporcionado para uma pessoa singular.

O regulamento não atribui às diferentes infrações um valor específico, apenas um limite (montante máximo). Tal pode indicar um grau de gravidade relativamente menor de uma violação das obrigações enumeradas no artigo 83.º, n.º 4, em relação às descritas no artigo 83.º, n.º 5. A reação efetiva, proporcionada e dissuasiva a uma violação do artigo 83.º, n.º 5, dependerá, contudo, das circunstâncias do caso.

[7] A avaliação da sanção a aplicar poderá ocorrer em separado, após a determinação da existência de infração por força de normas processuais nacionais decorrentes dos requisitos constitucionais de alguns países. Por conseguinte, tal pode limitar, nesses países, o conteúdo e o nível de detalhe de um projeto de decisão emitido pela autoridade de controlo principal.

Note-se que violações do regulamento que, pela sua natureza, possam enquadrar-se na categoria de *«até 10 000 000 EUR ou [...] até 2 % do seu volume de negócios anual a nível mundial»*, como prevê o artigo 83.º, n.º 4, podem acabar por ser incluídas, em certas circunstâncias, numa categoria de limiar mais elevado (20 milhões de EUR). Poderá ser este o caso quando tais violações já tiverem sido objeto de uma ordem emitida pela autoridade de controlo, ordem[8] essa que o responsável pelo tratamento ou subcontratante não tiverem cumprido[9] (artigo 83.º, n.º 6). As disposições do direito nacional podem, na prática, ter impacto nesta avaliação[10]. A natureza da infração, mas também *«o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos»*, serão reveladores da **gravidade** da infração. A ocorrência de várias infrações distintas, cometidas em conjunto em qualquer caso individual específico, significa que a autoridade de controlo pode aplicar as coimas a um nível que seja efetivo, proporcionado e dissuasivo, dentro do limite aplicável à infração mais grave. Por conseguinte, se for identificada uma infração aos artigos 8.º e 12.º, a autoridade de controlo poderá aplicar as medidas corretivas estabelecidas no artigo 83.º, n.º 5, que correspondam à categoria da infração mais grave, a saber, a do artigo 12.º. Nesta fase, um maior detalhe não se insere no âmbito desta diretriz específica (visto que o trabalho de cálculo detalhado constituirá o foco de uma eventual fase posterior desta diretriz).

Os fatores abaixo indicados devem ser avaliados conjuntamente, nomeadamente o número de titulares de dados juntamente com os eventuais efeitos para eles.

O número de titulares de dados envolvidos deve ser avaliado, a fim de identificar se se trata de um acontecimento isolado ou se indicia uma violação mais sistémica ou a falta de rotinas adequadas. O que precede não implica que acontecimentos isolados não sejam alvo de medidas, uma vez que podem, não obstante, afetar um número elevado de titulares de dados. Consoante as circunstâncias do caso, a relevância desse número estará relacionada, por exemplo, com o número de inscritos na base de dados em questão, o número de utilizadores de um serviço, o número de clientes ou a população do país, conforme o caso.

---

[8] As ordens, estabelecidas no artigo 58.º, n.º 2, são:

- Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento;
- Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado;
- Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais;
- Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;
- Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16.º, 17.º e 18.º, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17.º, n.º 2, e do artigo 19.º;
- Ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42.º e 43.º, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos;
- Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

[9] A aplicação do artigo 83.º, n.º 6, deve forçosamente ter em conta o direito processual nacional. O direito nacional determina o modo de emissão e notificação das ordens, assim como o momento a partir do qual produzem efeitos, e se existe, ou não, um período de tolerância para fins de cumprimento. Deve ser tido em consideração, entre outros, o efeito de um recurso sobre o caráter executivo da ordem.

[10] As disposições legais em matéria de prescrição podem levar a que uma ordem emitida pela autoridade de controlo deixe de ser tida em consideração em virtude do período decorrido desde a emissão da mesma. Em alguns países existem normas que determinam que, decorrido o prazo de prescrição da ordem, não pode ser imposta qualquer coima pelo seu incumprimento nos termos do artigo 83.º, n.º 6. Incumbirá às autoridades de controlo de cada país determinar os efeitos nacionais de uma situação deste tipo.

A finalidade do tratamento de dados deve igualmente ser avaliada. O parecer do Grupo do Artigo 29.º sobre a «limitação da finalidade»[11] já analisou os dois principais elementos de base deste princípio na legislação de proteção de dados: especificação da finalidade e utilização compatível. Ao avaliar a finalidade do tratamento de dados no contexto do artigo 83.º, n.º 2, as autoridades de controlo devem examinar em que medida esse tratamento respeita os dois elementos-chave deste princípio[12]. Em determinadas situações, a autoridade de controlo pode considerar necessária a inclusão de uma análise mais aprofundada da finalidade do tratamento de dados na análise a que se refere o artigo 83.º, n.º 2.

Se os titulares dos dados tiverem sofrido **danos**, o nível dos danos tem de ser tomado em consideração. O tratamento de dados pessoais pode gerar riscos para os direitos e liberdades das pessoas, segundo o considerando 75:

> *«O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial: quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízo significativo de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou dados relativos à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.»*

Se, devido à infração ao regulamento, tiverem sido ou seja expectável que venham a ser sofridos danos, a autoridade de controlo deve ter esse elemento em conta ao escolher a medida corretiva, embora a autoridade não seja competente para atribuir a indemnização pelos danos sofridos.

A imposição de uma coima não depende da capacidade da autoridade de controlo para estabelecer um nexo de causalidade entre a violação e o prejuízo material (cf., por exemplo, art. 83.º, n.º 6).

A **duração** da infração pode indicar, por exemplo:

a) Conduta deliberada por parte do responsável pelo tratamento; ou

b) Ausência de medidas preventivas adequadas; ou

c) Incapacidade de adotar as medidas técnicas e organizativas necessárias.

b) O caráter intencional ou negligente da infração

Geralmente, a «intenção» inclui tanto conhecimento como vontade, no que se refere às características da violação, ao passo que a «negligência» significa que não houve intenção de provocar a infração,

[11] WP 203, Parecer 03/2013 sobre a limitação da finalidade, disponível em: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf .
[12] Cf. também WP 217, Parecer 06/2014 sobre o conceito de interesse legítimo do responsável pelo tratamento nos termos do artigo 7.º, pág. 24, no que se refere à questão: *«O que torna um interesse 'legítimo' ou 'ilegítimo'?»*

embora o responsável pelo tratamento/subcontratante tenha violado o dever de diligência exigido por lei.

É geralmente reconhecido que as violações intencionais, que revelam incumprimento da lei, são mais graves do que as negligentes, sendo, por conseguinte, mais expectável que justifiquem a aplicação de uma coima. As conclusões relativas à intenção ou negligência resultarão dos elementos de conduta objetivos determinados a partir dos factos do caso. Além disso, a jurisprudência e a prática emergentes no domínio da proteção de dados no âmbito da aplicação do regulamento fornecerão exemplos de circunstâncias que indicam limiares mais claros para apreciar a intencionalidade da violação.

Circunstâncias reveladoras de violações intencionais podem ser o tratamento ilícito explicitamente autorizado pelos quadros superiores do responsável pelo tratamento, ou o tratamento que ignore aconselhamento do encarregado da proteção de dados ou as políticas existentes, como, por exemplo, a obtenção e tratamento de dados sobre funcionários de um concorrente com a intenção de desacreditar esse concorrente no mercado.

Outros exemplos são:

- a alteração de dados pessoais para fazer passar uma impressão enganadora (positiva) relativamente à consecução de metas – o que já aconteceu no contexto de metas relativas aos tempos de espera hospitalares
- a venda de dados pessoais para fins de comercialização, ou seja, a sua venda como se o titular tivesse dado o seu consentimento, sem verificar ou simplesmente desrespeitando a opinião dos titulares dos dados quanto à forma como os mesmos devem ser utilizados.

Outras circunstâncias, como a ausência de leitura e o desrespeito por políticas em vigor, erro humano, ausência de verificação da existência de dados pessoais em informações publicadas, ausência de aplicação tempestiva de atualizações técnicas, ausência de adoção de políticas (mais do que a mera ausência de aplicação das mesmas) podem igualmente ser reveladoras de negligência.

As empresas devem ser responsáveis pela criação de estruturas e recursos adequados à natureza e complexidade das suas atividades. Como tal, os responsáveis pelo tratamento e os subcontratantes não podem invocar a falta de recursos para legitimar violações da legislação de proteção de dados. As rotinas e a documentação de atividades de tratamento de dados seguem uma abordagem baseada nos riscos, em conformidade com o regulamento.

Existem zonas cinzentas que incidirão sobre a tomada de decisões quanto à eventual imposição de medidas corretivas, podendo a autoridade necessitar de realizar uma investigação mais aprofundada para apurar os factos do caso concreto e garantir que todas as circunstâncias específicas foram suficientemente tomadas em consideração.

c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares

Os responsáveis pelo tratamento dos dados e os subcontratantes têm a obrigação de aplicar medidas técnicas e organizativas que garantam um nível de segurança adequado ao risco, assim como de realizar avaliações do impacto em matéria de proteção de dados e atenuar os riscos para os direitos e liberdades das pessoas decorrentes do tratamento de dados pessoais. Contudo, sempre que ocorrer uma violação e o titular dos dados sofrer danos, a parte responsável deve envidar todos os esforços para limitar as consequências da violação para a(s) pessoa(s) em causa. Esse comportamento responsável (ou a ausência do mesmo) será tido em conta pela autoridade de controlo na escolha da(s) medida(s) corretiva(s), bem como no cálculo da sanção a impor no caso específico.

Embora os fatores agravantes ou atenuantes sejam particularmente adequados para ajustar o montante de uma coima às circunstâncias específicas do caso, o papel que desempenham na escolha da medida

corretiva adequada não deve ser subestimado. Nos casos em que uma avaliação baseada noutros critérios deixar a autoridade de controlo com dúvidas em relação à adequação de uma coima, quer enquanto medida corretiva aplicada isoladamente, quer em combinação com outras medidas do artigo 58.º, tais circunstâncias agravantes ou atenuantes podem ajudar a escolher as medidas apropriadas, fazendo a balança pender a favor da medida que se afigurar mais efetiva, proporcionada e dissuasiva no caso em apreço.

Esta disposição funciona como uma avaliação do grau de responsabilidade do responsável pelo tratamento após a ocorrência da infração. Pode abranger casos em que o responsável pelo tratamento/subcontratante não tenha manifestamente dado provas de uma abordagem imprudente/negligente, mas sim feito tudo ao seu alcance para emendar as suas ações quando tomou conhecimento da infração.

A experiência reguladora das autoridades de controlo no âmbito da aplicação da Diretiva 95/46/CE já revelou que pode ser adequado conceder um certo grau de flexibilidade aos responsáveis pelo tratamento de dados/subcontratantes que admitirem a infração e assumirem responsabilidade pela correção ou limitação dos efeitos dos seus atos. Exemplos disso são (embora nem sempre tal conduza a uma abordagem mais flexível):

- o contacto com outros responsáveis pelo tratamento/subcontratantes que possam ter estado envolvidos numa parte do tratamento, por exemplo se tiverem sido indevidamente partilhados dados com terceiros.
- a tomada de medidas atempada por parte do responsável pelo tratamento de dados/subcontratante para pôr cobro à infração ou impedir que esta evolua para um nível ou fase que teria efeitos bem mais graves.

d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º

O regulamento introduziu um nível bastante mais elevado de responsabilidade do responsável pelo tratamento de dados em comparação com a Diretiva 95/46/CE relativa à proteção de dados.

O grau de responsabilidade do responsável pelo tratamento ou do subcontratante, avaliado com vista à aplicação de uma medida corretiva adequada, pode incluir os seguintes aspetos:

- O responsável pelo tratamento aplicou medidas técnicas que respeitam os princípios da proteção de dados desde a conceção e por defeito (art. 25.º)?
- O responsável pelo tratamento aplicou medidas organizativas que dão cumprimento aos princípios da proteção de dados desde a conceção e por defeito (art. 25.º) a todos os níveis da organização?
- O responsável pelo tratamento/subcontratante aplicou um nível adequado de segurança (art. 32.º)?
- As rotinas/políticas pertinentes de proteção de dados são conhecidas e aplicadas no nível adequado de gestão da organização (art. 24.º)?

Os artigos 25.º e 32.º do regulamento exigem que os responsáveis pelo tratamento tenham em conta *«as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares»*. Mais do que representarem uma obrigação em termos de metas, estas disposições preveem obrigações relativas a meios, ou seja, o responsável pelo tratamento tem de realizar as avaliações necessárias e extrair as conclusões adequadas. A questão à qual a autoridade de controlo deve dar resposta é a de saber em que medida é que o responsável pelo tratamento «fez aquilo que era expectável que fizesse» atendendo à natureza, finalidades ou dimensão do tratamento, à luz das obrigações que lhe incumbem por força do regulamento.

Nesta avaliação, devem ser tidos em devida conta, sempre que existam e sejam aplicáveis, quaisquer procedimentos ou métodos que constituam «boas práticas». É importante ter em conta as normas do setor, bem como códigos de conduta da área de atividade ou profissão em causa. Os códigos deontológicos podem incluir indicações sobre práticas correntes na área de atividade e o nível de conhecimentos acerca de diferentes meios para resolver questões de segurança normalmente associadas ao tratamento de dados.

Embora, no geral, a boa prática represente o ideal a atingir, na avaliação do grau de responsabilidade devem ser tidas em conta as circunstâncias especiais de cada caso.

e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante

Este critério destina-se a avaliar o histórico da entidade no que se refere à ocorrência da infração. Neste contexto, as autoridades de controlo devem ter em conta que o âmbito da avaliação pode ser bastante alargado, pois qualquer tipo de violação do regulamento, ainda que de natureza distinta daquela que está a ser investigada pela autoridade de controlo, pode ser «pertinente» para essa avaliação, uma vez que pode ser reveladora de um nível geral de conhecimentos insuficientes ou de desrespeito pelas normas de proteção de dados.

A autoridade de controlo deve avaliar o seguinte:

- O responsável pelo tratamento/subcontratante cometeu a mesma infração anteriormente?
- O responsável pelo tratamento/subcontratante cometeu uma infração ao regulamento nas mesmas condições? (por exemplo, em resultado de conhecimentos insuficientes sobre as rotinas em vigor na organização, de uma avaliação dos riscos inadequada, de não responder atempadamente a pedidos do titular dos dados, de atrasos injustificados na resposta a pedidos, e assim por diante).

f) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos

O artigo 83.º, n.º 2, estabelece que o grau de cooperação pode ser tido em *«devida consideração»* ao decidir impor uma coima e determinar o seu montante. O regulamento não prevê expressamente a forma como devem ser tidos em conta os esforços dos responsáveis pelo tratamento ou subcontratantes para sanar uma infração já estabelecida pela autoridade de controlo. Além disso, deixa claro que os critérios devem ser habitualmente aplicados ao cálculo do montante da coima a impor.

Contudo, nos casos em que a intervenção do responsável pelo tratamento tiverem levado a que as consequências negativas para os direitos das pessoas não se materializassem ou tivessem um impacto mais limitado do que teriam tido de outra forma, essa intervenção também pode ser tida em conta na escolha de uma medida corretiva proporcionada ao caso concreto.

Um exemplo de um caso no qual pode ser pertinente ter em consideração a cooperação com a autoridade de controlo é o seguinte:

- No que se refere, nesse caso específico, aos pedidos da autoridade de controlo durante a fase de investigação, a entidade respondeu de uma forma que limitou significativamente o impacto para os direitos das pessoas?

Posto isto, não seria adequado atribuir uma importância adicional à cooperação que já é exigida por lei, como, por exemplo, se já for exigido à entidade que permita que a autoridade de controlo aceda às suas instalações para a realização de auditorias/inspeções.

g) As categorias específicas de dados pessoais afetadas pela infração

Eis alguns exemplos de perguntas-chave às quais a autoridade de controlo pode, neste contexto, e se pertinente para o caso, considerar necessário responder:

- A infração diz respeito ao tratamento das categorias especiais de dados previstas nos artigos 9.º e 10.º do regulamento?
- Os dados são diretamente identificáveis/indiretamente identificáveis?
- O tratamento envolve dados cuja divulgação poderia causar danos/inconvenientes imediatos à pessoa em causa (dados não abrangidos pelas categorias dos artigos 9.º ou 10.º)?
- Os dados estão diretamente acessíveis sem proteções técnicas, ou estão cifrados[13]?

h) A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, a medida em que o fizeram

A autoridade de controlo pode tomar conhecimento da infração na sequência de uma investigação, de reclamações, de artigos de imprensa, de denúncias anónimas ou de uma notificação por parte do responsável pelo tratamento de dados. Nos termos do regulamento, o responsável pelo tratamento tem a obrigação de comunicar as violações de dados pessoais à autoridade de controlo. Nos casos em que o responsável pelo tratamento se limita a cumprir a sua obrigação, tal cumprimento não pode ser interpretado como fator atenuante. Do mesmo modo, o responsável pelo tratamento de dados/subcontratante que tiver agido com negligência, não procedendo à notificação, ou pelo menos não notificando todos os detalhes da infração, por não ter avaliado adequadamente a dimensão da infração, pode igualmente merecer sanção mais grave por parte da autoridade de controlo, ou seja, é improvável que a infração seja considerada menor.

i) O cumprimento das medidas a que se refere o artigo 58.º, n.º 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria

A autoridade de controlo poderá já ter assinalado um responsável pelo tratamento ou subcontratante, para efeitos de supervisão da respetiva conformidade, na sequência de uma infração anterior e quando é presumível que, se for caso disso, os contactos com o encarregado da proteção de dados tenham sido significativos. Por conseguinte, a autoridade de controlo terá em conta os contactos anteriores.

Contrariamente ao critério constante da alínea e), este critério de avaliação destina-se somente a remeter as autoridades de controlo para as medidas que elas próprias já tiverem aplicado previamente ao mesmo responsável pelo tratamento ou subcontratante *«relativamente à mesma matéria»*.

j) O cumprimento de códigos de conduta aprovados nos termos do artigo 40.º ou de procedimentos de certificação aprovados nos termos do artigo 42.º

As autoridades de controlo têm o dever de *«[controlar] e [executar] a aplicação do presente regulamento»* [art. 57.º, n.º 1, alínea a)]. A observância de códigos de conduta aprovados pode ser utilizada pelo responsável pelo tratamento/subcontratante como forma de demonstrar a conformidade, de acordo com os artigos 24.º, n.º 3, 28.º, n.º 5, ou 32.º, n.º 3.

Em caso de violação de uma das disposições do regulamento, a observância de um código de conduta aprovado pode igualmente ser reveladora de quão profunda é a necessidade de a autoridade controlo

[13] Não se deve considerar um fator atenuante «extra» o facto de a violação só dizer respeito a dados indiretamente identificáveis ou a dados pseudonimizados/cifrados. No que se refere a tais violações, uma avaliação global dos restantes critérios pode fornecer uma indicação moderada ou forte de que deve ser imposta uma coima.

intervir através de uma coima que seja efetiva, proporcionada e dissuasiva ou através de outra medida corretiva. Os códigos de conduta aprovados devem, de acordo com o artigo 40.º, n.º 4, prever «*procedimentos que permitam ao organismo [de supervisão] [...] efetuar a supervisão obrigatória do cumprimento das suas disposições*».

Nos casos em que o responsável pelo tratamento ou o subcontratante observem um código de conduta aprovado, a autoridade de controlo pode considerar suficiente que a comunidade do código, encarregada da sua aplicação, imponha, ela mesma, as medidas adequadas ao membro, por exemplo, através de mecanismos de supervisão e execução do próprio código de conduta. Por conseguinte, a autoridade de controlo pode considerar que, nesse caso específico, tais medidas são suficientemente efetivas, proporcionadas ou dissuasivas, sem que haja necessidade de a autoridade de controlo impor medidas adicionais. Certas sanções por comportamentos não conformes podem ser aplicadas através do mecanismo de supervisão, em conformidade com o artigo 41.º, n.º 2, alínea c), e n.º 4, incluindo a suspensão ou exclusão do responsável pelo tratamento ou do subcontratante em causa da comunidade do código. Contudo, as competências do organismo de supervisão não prejudicam as *«funções e competências da autoridade de controlo competente»*, o que significa que a autoridade de controlo não é obrigada a ter em conta sanções previamente impostas através do mecanismo de autorregulação.

O incumprimento de medidas de autorregulação também pode revelar negligência ou comportamento intencionalmente desconforme por parte do responsável pelo tratamento/subcontratante.

k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração

A própria disposição fornece exemplos de quais os outros elementos que podem ser tidos em conta na decisão sobre a adequação de uma coima relativamente a uma infração ao artigo 83.º, n.os 4 a 6.

As informações acerca de lucros obtidos em resultado de uma violação podem revestir-se de especial importância para as autoridades de controlo, uma vez que um ganho económico decorrente da infração não pode ser compensado através de medidas que não incluam uma componente pecuniária. Como tal, o facto de o responsável pelo tratamento ter lucrado com a infração ao regulamento pode constituir um forte indício de que deve ser aplicada uma coima.

IV. Conclusão

As reflexões sobre as questões referidas na secção anterior ajudarão as autoridades de controlo a identificar, a partir dos factos pertinentes do caso, os critérios mais úteis para tomarem uma decisão relativa à eventual imposição de uma coima adequada que complemente ou substitua outras medidas nos termos do artigo 58.º. Tendo em conta o contexto fornecido por essa avaliação, a autoridade de controlo identificará a medida corretiva mais efetiva, proporcionada e dissuasiva para dar resposta à violação.

O artigo 58.º faculta algumas orientações quanto às medidas que as autoridades de controlo podem escolher, uma vez que as medidas corretivas são, em si mesmas, de diferentes naturezas e primariamente indicadas para alcançar fins distintos. Algumas das medidas previstas no artigo 58.º podem até ser cumulativas, obtendo-se desse modo uma ação reguladora composta por mais de uma medida corretiva.

Nem sempre é necessário complementar a medida recorrendo a outra medida corretiva. Por exemplo: a efetividade e o caráter dissuasivo da intervenção da autoridade de controlo, com a devida consideração

daquilo que é proporcionado nesse caso específico, podem ser alcançados através da mera aplicação da coima.

Em suma, as autoridades têm de restabelecer a conformidade por meio de todas as medidas corretivas à sua disposição. As autoridades de controlo também deverão escolher a via mais adequada para a prossecução da ação reguladora. Tal pode, por exemplo, incluir sanções penais (se previstas a nível nacional).

A prática de aplicar coimas de forma coerente em toda a União Europeia é uma arte em desenvolvimento. As autoridades de controlo devem colaborar no sentido de aumentar continuamente a coerência das medidas. Tal pode ser alcançado através de intercâmbios regulares, seminários de tratamento de casos ou outros eventos que permitam a comparação de casos a nível regional, nacional e transnacional. Recomenda-se a criação de um subgrupo permanente ligado aos elementos do CEPD responsáveis por esta matéria, a fim de apoiar esta atividade contínua.