REVISTA DE DIREITO COMERCIAL

Covid-19 e plataformas de *streaming*: breve reflexão

Mafalda Miranda Barbosa[1]

1. Introdução

A pandemia de covid-19 fez emergir inúmeros problemas sanitários, sociais, económicos e também jurídicos. Um dos aspetos que, do ponto de vista do direito, se torna problemático diz respeito à proteção de dados pessoais. A conexão pode não ser imediatamente percetível e pode, inclusivamente, passar despercebida, pelo menos num primeiro momento em que a urgência se coloca na necessidade de conter a progressão da doença e dos contágios. Mas não deixa de ser real e de levantar problemas interessantes e de nem sempre fácil resolução.

Numa primeira abordagem, podemos adiantar que a ameaça aos dados pessoais (e à proteção que genericamente lhe é dispensada) conhece uma dupla origem. Por um lado, pode resultar da necessidade de os poderes públicos (policiais, sanitários ou outros) ou entidades privadas (por indicação daquelas) adotarem as medidas de contenção a que já fizemos referência; por outro lado, surge na sequência dos novos hábitos que foram sendo adotados para

[1] Univ Coimbra, Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra/University of Coimbra Institute for Legal Research, Faculdade de Direito da Universidade de Coimbra

satisfazer necessidades primordiais da população confinada (maioritariamente) ao seu domicílio.

A intencionalidade dos problemas patenteados por cada uma destas origens não é idêntica e não pode receber uma resposta unívoca. Por isso, centrando-nos preferencialmente naquelas hipóteses que se mostram mais próximas dos campos dogmáticos que temos cultivado, procuraremos, não obstante, traçar a diferença entre ambos os nichos problemáticos.

2. O duplo desafio à proteção de dados

Se justificadamente aceitamos que o surto epidémico que se enfrenta coloca desafios à proteção de dados a diversos níveis, importa começar por apresentar a bifurcação a que se aludiu previamente.

Assim, num primeiro nível, não sendo o vírus em si que determina a lesão do direito à proteção de dados, esta pode emergir por via de algumas soluções que os Estados oferecem para dar resposta à doença. No horizonte assomam três situações problemáticas (embora outras se pudessem cogitar): a utilização de *drones* para vigilância dos obrigados à quarentena; a recolha e partilha de dados relativos à saúde dos cidadãos; a utilização de aplicações de telemóvel que, com base em dados de geolocalização e biométricos ou em metadados, permitem controlar eventuais deslocações e sintomas das pessoas e alertar as restantes, sempre que tenham estado em contacto com algum infetado ou suspeito de infeção. Neste âmbito, como veremos, podendo ser facilmente discernível

um fundamento para o tratamento de dados em si mesmo, o problema centra-se no cumprimento dos requisitos de licitude daquele. Designadamente, o nódulo central das questões juridicamente relevantes situar-se-á no controlo do conteúdo do tratamento de que se cura. Ideias como a minimização dos dados, a proporcionalidade e a adequação, a fazer articular as regras próprias da proteção de dados com a arquitetura constitucional vigente no ordenamento jurídico português, tornam-se então atuantes.

Num segundo nível, não está em causa um atentado direto (embora possivelmente justificado, dentro de determinados limites) ao direito à proteção de dados pessoais por parte de entidades públicas, no sentido de conter a propagação da doença, mas eventuais lesões daquele direito fundamental como consequência indireta de medidas adotadas no quadro da emergência sanitária. Neste âmbito, as questões são, como veremos, outras. O núcleo central de problematicidade já não se situa no cumprimento ou não de princípios como a minimização dos dados ou da proporcionalidade e adequação, sequer na adoção de salvaguardas que garantam a não discriminação ou a restrição desmedida dos direitos que subjazem ao direito à tutela dos dados pessoais, mas no próprio caráter lícito ou ilícito do tratamento, ou seja, na existência ou inexistência de um fundamento de legitimação para o tratamento de que se cura.

3. A proteção de dados em tempo de covid-19: o combate à pandemia

Perante a possibilidade de utilização de *drones* para vigilância da população, do acesso a metadados, a dados biométricos e de geolocalização por parte das autoridades sanitárias, o atentado contra o direito à proteção de dados, na base do qual encontramos outros direitos de personalidade (em termos publicistas, qualificados como direitos fundamentais), é evidente. Nem por isso, porém, se pode concluir que o tratamento de dados que tais comportamentos envolvem sejam ilícitos.

Na verdade, o artigo 6º/1/d) RGPD integra, entre os fundamentos de legitimação do tratamento de dados, o facto de tal tratamento ser necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular. As circunstâncias potenciadas pela covid-19, associadas a eventuais declarações de estado de emergência[2], podem, em teoria, ser assimiladas pelo âmbito de relevância do preceito. Mesmo tratando-se de dados sensíveis – alguns dos quais atinentes à saúde dos sujeitos –, o artigo 9º/2/i) RGPD autoriza o seu tratamento, se ele for necessário por motivos de interesse público no domínio da saúde pública. Neste contexto, aliás, o *Considerandum* 46 refere-se aos tratamentos de dados legitimados "para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial situações de catástrofes naturais ou de origem humana".

Fundamental será, para se concluir justificadamente pela legitimação do tratamento, que ele se afigure necessário. Esta necessidade – atentos os valores em causa – não pode equivaler à

[2] Teceremos, *infra*, um breve comentário acerca do impacto que a declaração de estado de emergência pode ter em sede de proteção de dados.

mera aptidão das medidas para lidar com o surto epidémico. Ao invés, deverá ser entendido no sentido de ser imperioso adotar os procedimentos em questão. É claro que o artigo 23º RGPD admite que os Estados membros limitem algumas das obrigações a que fica sujeito o responsável pelo tratamento de dados por motivos de interesse público, entre os quais se integra a saúde pública. Contudo, essa possibilidade não diz respeito aos fundamentos do tratamento, consoante se esclarece no nº2 do citado artigo 23º, pelo que não pode prescindir-se do controlo legitimador que seja imposto pelo critério da necessidade. Esta parece, de facto, ser a única posição defensável se tivermos em conta princípios fundamentais nesta matéria.

Por um lado, haveremos de ter em conta que subjacente ao direito à proteção de dados encontramos outros direitos fundamentais, em relação aos quais aquele funciona como guarda-avançada[3]. Ora, tratando-se de direitos com assento constitucional, a sua limitação há de obedecer também ela a limites precisos, que a doutrina tem vindo a sedimentar. Se, por exemplo, tivermos em conta o possível acesso aos dados de comunicações, estabelecendo o artigo 34º CRP que o sigilo dos meios de comunicação é inviolável, sendo proibida qualquer ingerência nas telecomunicações, não deixam de suscitar-se dúvidas acerca da bondade constitucional da solução. E se o

[3] Falando de uma relação de interioridade constitutiva, cf. Mafalda Miranda BARBOSA, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *Estudos de Direito do Consumidor*, 12, 2017, 75-132 (= "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *AB Instantia*, ano V, 7, 2017, 13-47)

problema poderia ser ultrapassado pela declaração do estado de emergência, importa considerar que, em concreto, o decreto que o estabeleceu não previu qualquer restrição ao direito à confidencialidade dos meios de comunicação privada, por um lado, e, por outro lado, que não fica anulado, nesse contexto, o princípio da proporcionalidade.

De facto, e já em articulação com os princípios fundamentais em matéria de proteção de dados, não obstante as restrições a que podemos ser conduzidos por via do artigo 23º RGPD, importa ter em conta o princípio da minimização. Dispõe o artigo 5º/1/c) RGPD que os dados pessoais recolhidos têm de ser adequados, pertinentes e limitados ao que seja necessário relativamente às finalidades para as quais são tratados, correspondendo à anterior norma do artigo 5º/1 c) Lei nº67/98. Significa isto que o tratamento de dados deve obedecer a uma ideia de proporcionalidade. Ora, é precisamente essa ideia que pode ficar comprometida com algumas das medidas adotadas para fazer face ao surto pandémico, se elas não se revelarem imprescindíveis (e não meramente aptas).

Sem nos querermos alargar neste tópico, sempre haveremos de dizer, por exemplo, que o acesso a metadados através de aplicativos telefónicos que visassem determinar os movimentos e identificar os contactos das pessoas para garantir a sequenciação de eventuais cadeias de transmissão da doença pode pôr em causa o princípio da minimização a que nos referimos. Basta para tanto que se conclua, por exemplo, que tal acesso não é necessário, por não ser imperioso, podendo alcançar-se o mesmo objetivo através do acesso a dados anónimos por *bluebooth*. Igualmente problemática pode ser a utilização de dados biométricos associados a tais dados de geolocalização.

Ao nível europeu, a Comissão Europeia recomendou, neste contexto, que fossem desenvolvidas estratégias comuns na resposta à pandemia que poderiam passar pelo uso de aplicações móveis e dados móveis, entre as quais se conta o uso de aplicações móveis para reforçar o cumprimento do distanciamento social por parte dos cidadãos e garantir o aviso e a prevenção de contactos com infetados; bem como o desenvolvimento de um modelo preditivo de evolução do vírus e sua disseminação, através de dados móveis anónimos e agregados. Se, ao serem anonimizados, os dados perdem a sua natureza de dados pessoais, o mesmo não se diga dos dados tratados para efeitos de rastreamento do cumprimento do isolamento imposto e da análise de sintomas/alerta de contacto com um infetado.

A Comissão Europeia, contudo, mostra-se particularmente preocupada em prosseguir uma política de proteção de dados pessoais. A *Commission Recommendation of 8-4-2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data* [C (2020) 2296][4] evidencia isso mesmo.

No Quadro da Recomendação C (2020) 2296, e para salvaguarda da privacidade e da proteção de dados, a ferramenta que seja desenvolvida deve limitar estritamente o processamento de dados às finalidades de combate à covid-19, assegurando-se que os referidos dados não serão usados para nenhum outro propósito, incluindo

[4] https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_ contact_tracing_4.pdf

objetivos sancionatórios ou comerciais; deve limitar os dados ao estritamente necessário; deve assegurar que, logo que o procedimento deixe de ser estritamente necessário, os dados pessoais são destruídos irreversivelmente, a não ser que o seu valor científico ao serviço de interesses públicos supere o peso relativo dos direitos envolvidos. No que respeita especificamente ao uso de aplicações móveis de aviso e prevenção, devem ser observados diversos princípios:

> «safeguards ensuring respect for fundamental rights and prevention of stigmatization, in particular applicable rules governing protection of personal data and confidentiality of communications; preference for the least intrusive yet effective measures, including the use of proximity data and the avoidance of processing data on location or movements of individuals, and the use of anonymised and aggregated data where possible; technical requirements concerning appropriate technologies (e.g. *Bluetooth Low Energy*) to establish device proximity, encryption, data security, storage of data on the mobile device, possible access by health authorities and data storage; effective cybersecurity requirements to protect the availability, authenticity integrity, and confidentiality of data; the expiration of measures taken and the deletion of personal data obtained through these measures when the pandemic is declared to be under control, at the latest; uploading of proximity data in case of a confirmed infection and appropriate methods of warning

> persons who have been in close contact with the infected person, who shall remain anonymous; and transparency requirements on the privacy settings to ensure trust into the applications».

O *European Data Protection Board, na Letter concerning the European Commission's draft Guidance on apps supporting the fight against the COVID-19 pandemic*, de 15 de Abril de 2020[5], sublinha a necessidade de minimizar a interferência com a vida privada, ainda que se tenha de preservar a saúde pública. Além disso, apoia fortemente a proposta da comissão no sentido da adoção voluntária da aplicação. Apesar da importância do consentimento, o *European Data Protection Board* refere que o facto de haver uma base voluntária não significa que o tratamento dos dados pessoais pelas autoridades públicas se baseie necessariamente no consentimento. Quando aquelas autoridades públicas prestam um serviço, baseadas num mandato atribuído por lei ou em consonância com as determinações legais, parece que o fundamento que legitima o tratamento se encontrar na necessidade de salvaguardar o interesse público. A este propósito, importa, não obstante, ter em conta a diferença entre um modelo compulsório de implementação dos aplicativos e um modelo voluntário.

A ideia está, assim, em consonância com uma ideia de minimização de dados. A este princípio aliam-se outros que devem ser respeitados. Entre eles, saliente-se o *princípio da limitação da conservação* (os dados pessoais devem ser conservados de uma

[5] https://edpb.europa.eu/news/news/2020/twenty-first-plenary-session-european-data-protection-board-letter-concerning_pt

forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados), que reproduz sensivelmente a solução consagrada no artigo 5º/1 e) Lei nº67/98, embora se esclareça, agora, que os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos; e o *princípio da exatidão* (os dados pessoais devem ser exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora). Além disso, o processo de tratamento de dados deve obedecer a requisitos específicos, que garantam o cumprimento dos princípios a que os *controllers* estão vinculados, exceto se tais obrigações forem restringidas ao abrigo do artigo 23º RGPD.

Entre nós, a Comissão Nacional de Proteção de Dados teve já oportunidade de se pronunciar acerca de alguns problemas suscitados pela covid-19 e pelas medidas adotadas no sentido da contenção da epidemia. Quanto à captação de imagens por câmaras de videovigilância e por *drones*, a CNPD rejeitou o uso generalizado, embora abra as portas à sua utilização segundo critérios delimitados em termos geográficos. Em despacho datado de 1 de abril, refere-se que «é precisamente porque o país se encontra em estado de emergência, e alguns direitos fundamentais dos cidadãos estão a ser objeto de uma intervenção policial mais restritiva, que tem de ser assegurado um controlo atento da concreta atividade das forças de segurança pelo membro do Governo responsável». Por outro lado, porque «o estado de emergência decretado não alterou as

atribuições e as competências públicas, pelo que se mantêm centralizadas no Estado as funções de controlo de entrada e deslocação em território nacional», a CNPD veio considerar que está vedada à Administração Pública Local e às entidades privadas a utilização de meios de captação de imagens e som no espaço público para controlo das fronteiras e a prevenção e repressão de crimes no espaço público. O que se percebe, portanto, é que o estado de emergência não justifica, por si só, toda e qualquer limitação de direitos fundamentais.

Embora não esteja em causa o direto combate à epidemia, mas a tentativa de solucionar alguns problemas que o contexto social e económico por ela gerado possa fazer emergir, a CNPD é clara ao sublinhar que o estado de emergência não afeta a salvaguarda de direitos fundamentais. O dado articula-se de forma perfeita com as tomadas de posição ao nível comunitário: o RGPD mantêm-se vigente e, se é certo que a emergência sanitária e interesses de ordem pública podem determinar a necessidade de tratamentos especiais de dados – alguns dos quais sensíveis –, não é menos seguro que tal tratamento deve obedecer aos princípios ali plasmados, que garantam a segurança da privacidade dos sujeitos.

Também no tocante à recolha de dados de saúde dos trabalhadores, tidos como dados sensíveis, a CNPD reforça que a situação excecional e a necessidade de prevenção do contágio não legitimam sem mais a adoção de toda e qualquer medida por parte da entidade empregadora, não justificando, designadamente, a realização de atos que só as autoridades de saúde ou o próprio

trabalhador, num processo de auto-monitorização, podem praticar[6]. Significa isto que a urgência imposta pelo novo coronavírus – esteja ou não declarado o estado de emergência – não pode justificar toda e qualquer medida que afrontosamente colide com o direito à proteção de dados pessoais: ainda que se possam impor restrições, legitimando-se formas de tratamento, elas devem obedecer aos princípios impostos ao nível do RGPD.

4. A proteção de dados em tempo de covid-19: a adaptação do estilo de vida

No quadro do estado de emergência decretado na sequência da pandemia covid-19, ao qual se seguiu um estado de calamidade, foi determinada, ainda, a obrigatoriedade do teletrabalho. Implementada esta nova forma de cumprir as obrigações laborais, os sujeitos são levados a transferir algumas das suas atividades para plataformas de *streaming*, como o *Zoom* ou a *Microsoft Teams*. Trabalhadores dos mais diversos setores e pessoas de todas as idades (pense-se, por exemplo, nos alunos que se veem forçados a formas de ensino à distância) aderem ao mundo digital, que passa também a ser ponto de encontro de famílias e amigos, em face do confinamento ou isolamento sociais igualmente impostos. A própria Igreja Católica, no cumprimento das indicações sanitárias, determina que as celebrações Eucarísticas sejam transmitidas *online*,

[6] CNPD, *Orientações sobre recolha de dados de saúde dos trabalhadores* (23 de abril de 2020).

recorrendo muitas paróquias a plataformas de *streaming*. O recurso a tecnologias de informação e comunicação passa a fazer parte do quotidiano da maioria das pessoas.

Este acesso massificado às ditas plataformas de *streaming*, quer no âmbito profissional[7], quer no âmbito pessoal, arrasta consigo perigos que têm vindo a ser denunciados pelos especialistas na área. Estando envolvidos dados pessoais, recolhidos em grande quantidade, a CNPD elenca alguns dos riscos a que aludimos: risco de utilização indevida dos dados transferidos através das plataformas por parte dos responsáveis dos tratamentos, ou por subcontratantes que forneçam serviços dessas plataformas (por exemplo, em sistemas assentes em *cloud computing*); risco de falta de controlo

[7] Os problemas que o teletrabalho levanta para a proteção de dados pessoais ultrapassam as questões suscitadas pelas plataformas de *streaming*. Veja-se, a este propósito, CNPD, *Orientações sobre o controlo à distância em regime de teletrabalho* (17 de abril de 2020). Refere-se aí que, embora o empregador mantenha os poderes de direção e de controlo da execução da prestação laboral, não se permite a utilização de meios de vigilância à distância, com a finalidade de controlar o desempenho profissional do trabalhador, de acordo com os princípios da proporcionalidade e da minimização de dados, "uma vez que a utilização de tais meios implica uma restrição desnecessária e seguramente excessiva da vida privada do trabalhador". Fica, assim, proibida a utilização de *softwares* de rastreamento do tempo de trabalho e da inatividade, de registo de páginas web visitadas, a possibilidade de captação de imagens do ambiente de trabalho, mecanismos de controlo do documento em que se está a trabalhar, etc. Do mesmo modo, considera a CNPD que não é possível obrigar a que o trabalhador mantenha a câmara de vídeo permanentemente ligada, nem será de admitir a possibilidade de gravação de teleconferências entre o empregador e o trabalhador. Não se impede, porém, a utilização de mecanismos de registo dos tempos de trabalho. Nos exemplos oferecidos pelas orientações da CNPD, podem utilizar-se ferramentas que reproduzam o registo do início e do fim da atividade laboral.

dos dados pelos seus titulares, pela falta de transparência relativamente à forma de armazenamento, tratamento e eventuais subcontratações realizadas por fornecedores de soluções assentes em *cloud computing*; risco de definição de perfis ou avaliações, com base na informação observada da atividade dos utilizadores, com o consequente risco de discriminação; risco de decisões automatizadas assentes em sistemas de inteligência artificial que analisem o comportamento e desempenho dos utilizadores; risco de perda de confidencialidade dos dados, pela falta de segurança das comunicações com possibilidade de acesso não autorizada; risco de vigilância à distância com a finalidade de controlar o desempenho profissional dos cidadãos[8].

E nessa medida, formula, também, uma série de recomendações, para garantir a proteção dos dados pessoais envolvidos. Resulta do exposto que a utilização de plataformas de *streaming* não é considerada ilícita pela CNPD. De acordo com a autoridade portuguesa em matéria de proteção de dados, a tutela deverá centrar-se no controlo do tratamento de dados que seja feito.

Cremos, porém, que o problema não pode ser abordado de uma

[8] CNPD, *Orientações para utilização de tecnologias de suporte ao ensino à distância*, 2020, https://www.cnpd.pt/home/orientacoes/Orientacoes_tecnologias_de_suporte_ao_ensino_a_distancia.pdf. As formulações contidas em texto acompanham de muito perto, reproduzindo-as, as formulações da CNPD. São, contudo, pontualmente alteradas para se tornarem mais abrangentes. Na verdade, enquanto a CNPD circunscreve a sua análise à utilização de tecnologias de suporte ao ensino à distância, o nosso foco é mais alargado.

forma unívoca[9]. Pelo contrário, importa estabelecer algumas distinções. Em primeiro lugar, o atentado contra os dados pessoais pode provir da própria plataforma que os recolhe e trata (ou de um subcontratante) ou pode ser perpetrado por um terceiro, um *hacker*, que explora alguma vulnerabilidade do sistema; em segundo lugar, haveremos de diferenciar as situações de uso voluntário e pessoal daqueloutras de uso obrigatório e profissional.

Se o primeiro binómio pode colocar especiais problemas no que respeita à responsabilidade; o segundo suscita dificuldades no que respeita ao fundamento de licitude do tratamento.

De acordo com o RGPD (artigo 6º), o tratamento de dados pessoais *só é lícito se existir consentimento do seu titular ou, em alternativa, se se verificar uma das seguintes situações*: se 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; se o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; se 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; se 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

[9] Repetimos o que já anteriormente havíamos referido: a CNPD limita-se a analisar o problema circunscrevendo-o ao ensino à distância. A nossa abordagem é mais ampla, justificando assim as diferenciações que estabeleceremos em texto.

titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Estando em causa a *utilização pessoal e voluntária* das plataformas de *streaming* a que aludimos, podemos discernir (em avanço) dois possíveis fundamentos de licitude do tratamento de dados: o consentimento do titular e a necessidade para a execução de um contrato no qual o titular dos dados é parte (o fornecimento do serviço de comunicação à distância ou de partilha de ficheiros fica, necessariamente, dependente da recolha e tratamento de dados pessoais). Não se levantando aí um problema de maior, há que ter, no entanto, em conta que há toda uma panóplia de dados que podem ser inadvertidamente partilhados e que não são essenciais ao cumprimento das referidas obrigações/execução do contrato: basta pensar na exposição do domicílio, na possível recolha e análise de dados preditivos, no possível acesso e tratamento das informações partilhadas por via da plataforma. Não estando (ou podendo não estar) muitos destes dados abrangidos quer pelo consentimento, quer pelas necessidades impostas pela execução do contrato, poder-se-á levantar quanto a eles o problema da (i)licitude do tratamento.

Além disso, importa ter em mente que, não raro, se impõe a articulação entre os diversos fundamentos de legitimação do tratamento de dados.

Consoante esclarece o grupo de trabalho do artigo 29º, embora por referência ao anterior quadro normativo, não só existem diversos fundamentos de legitimação do tratamento de dados, como *a mesma situação de base pode convocar mais do que um fundamento de licitude*. A consciência deste pormenor é extremamente importante: na verdade, se cada fundamento se orienta por uma

finalidade concreta, a mobilização de um deles não legitima o responsável a tratar os dados para lá dessa finalidade. Nessa medida, pode ser necessário convocar, no que respeita ao tratamento suplementar, o consentimento. Assim, por exemplo, se o tratamento de dados for necessário para a execução dos contratos em questão, ele é autorizado pelo artigo 6º/1 b) RGPD. Ao invocar-se este fundamento não se pode ir além do que é necessário, de acordo com a finalidade que preside ao fundamento, o que significa que, se o contraente pretender tratar os dados para outros fins, deverá obter o devido consentimento específico[10]. Ou seja, para a mesma situação de facto, confluem diversos fundamentos de legitimação do tratamento. Do mesmo modo, se em causa estão mais dados do que aqueles que são imprescindíveis à prestação do serviço/execução do contrato, quanto a estes deve exigir-se o consentimento. A questão passa, então, por garantir o estrito cumprimento do princípio da limitação das finalidades e da minimização dos dados.

Ou seja, se em causa estiverem dados necessários para a execução de um contrato (ou mesmo para a sua celebração), pode prescindir-se do consentimento; mas, em relação a dados não imprescindíveis e a outras finalidades, poder-se-á ter de exigir o consentimento. E, nos termos do artigo 13º/1 c) e do artigo 14º/1 c), o responsável pelo tratamento de dados deve informar o titular dos dados acerca do fundamento desse tratamento, antes de ele iniciar e relativamente a uma finalidade específica. Ora, consoante esclarece o grupo de trabalho do artigo 29º, "o responsável pelo tratamento, se optar por

[10] Parecer do grupo de trabalho do artigo 29º 15/2011, adotado em 13 de julho de 2011, 9 s. Explica-se, aí, que, na prática, se poderá ter de obter o consentimento como uma condição adicional para uma certa do tratamento.

invocar o consentimento para qualquer parte do tratamento, deve estar preparado para respeitar essa opção e parar essa parte do tratamento se um indivíduo retirar o consentimento (…). não pode passar do consentimento para outros fundamentos legais. Por exemplo, não lhe é permitido utilizar retroativamente o fundamento do interesse legítimo para justificar o tratamento, se forem detetados problemas com a validade do consentimento"[11]. Inversamente, não é possível invocar a necessidade de tratamento dos dados para a execução do contrato se em causa estiverem dados que ultrapassam essa finalidade. As plataformas de *streaming* devem, por exemplo, garantir que não seja captada a imagem/vídeo do utilizador, exceto se ele expressamente o consentir[12], devem garantir que a gravação dos conteúdos seja previamente autorizada, *et cetera*.

Estas ideias mostram-nos que, mesmo sendo imprescindível o tratamento de certos dados para a execução do contrato, pode ser necessário recolher o consentimento dos usurários da plataforma em relação a outros. E, se o consentimento surge como fundamento da legitimação do tratamento de certos dados, então ele tem de situar-se antes do início desse tratamento. Sendo o *quando* fácil de determinar, no que respeita ao *como*, às suas modalidades e à forma

[11] Orientações do grupo de trabalho do artigo 29º relativas ao consentimento na aceção do Regulamento (UE) 2016/679, 26.

[12] Tratando-se, porém, de um evento público (p. exemplo, uma conferência transformada numa webinar) coloca-se o problema de saber se poderá excluir-se a necessidade do consentimento no que respeita ao direito à imagem, nos termos do artigo 79º/2 CC. Mas já não parece ser de prescindir o consentimento do ponto de vista da proteção de dados.

que deve revestir, maiores dificuldades emergem.

No quadro da anterior disciplina, entendia-se que consentimento devia ser *dado de forma inequívoca*. Isto não significava, porém, que ele não pudesse ser *tácito*. Nos termos do artigo 217º CC, as declarações de vontade podem ser expressas ou tácitas, salvo determinação legal em contrário. Ora, sendo certo que não estaremos necessariamente (e em todas as hipóteses) diante de declarações negociais, o artigo 295º CC manda aplicar aos atos jurídicos que não sejam negócios jurídicos as disposições próprias destes, desde que a analogia das situações o justifique. O caráter inequívoco do consentimento não era posto em causa pela natureza concludente do comportamento que o consubstanciasse, tanto mais que o citado artigo 217º CC define a declaração tácita como aquela que "se deduz de factos que, com toda a probabilidade, a revelam". O grupo de trabalho do artigo 29º vinha admitir expressamente qualquer forma para o consentimento, embora se afastassem as omissões. Falava-se, entre outras, da assinatura de um formulário, de declarações orais, de um comportamento concludente, do envio de um pedido de informações, na medida em que o consentimento fosse necessário para lhe dar resposta[13]. O caráter expresso do consentimento só era exigível quando se lidasse com categorias especiais de dados, considerados sensíveis.

Nos termos do artigo 7º RGPD, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais. Ademais, se o consentimento do titular dos dados for dado no contexto de uma

[13] Parecer do grupo de trabalho do artigo 29º 15/2011, 13-14

declaração escrita que diga também respeito a outros assuntos, *o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples*. Onde a Lei nº67/98 falava de consentimento inequívoco, colocando-se o problema de saber se ele poderia ser tácito e chegando-se à conclusão que o caráter não expresso da declaração, nos termos do artigo 217º CC, não contrariava a inequivocidade dele, diz-se agora que *o responsável deve poder demonstrar que o titular dos dados deu o seu consentimento*. Trata-se de uma questão probatória, que não pode ser confundida com a modalidade da declaração em causa. Em rigor, mesmo que se exigisse que o consentimento fosse prestado segundo uma determinada forma – algo que o regulamento não dispõe –, nos termos do artigo 217º/2 CC, tal caráter formal não impediria que ela fosse emitida tacitamente, desde que a forma tivesse sido observada quanto aos factos de que a declaração se possa deduzir.

Haverá, contudo, de ter em conta o artigo 4º/11 Regulamento. Neste define-se o consentimento como "uma manifestação de vontade, *livre, específica*, *informada* e *explícita*, pela qual o titular dos dados aceita, *mediante declaração ou ato positivo inequívoco*, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[14]. Embora haja alusão à natureza explícita da manifestação da vontade, o regulamento afirma que esta tem lugar mediante declaração ou ato positivo inequívoco. A dualidade a que

[14] O artigo 3º/h) Lei nº67/98 não falava de manifestação explícita, limitando-se a definir o consentimento como ‘‘qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento".

assim somos conduzidos parece depor no sentido da admissibilidade de um comportamento concludente, desde que inequívoco e explícito. Simplesmente, se é de admitir, à luz do ordenamento jurídico português, e atenta a amplitude com que se compreendem os comportamentos declarativos, que haja consentimento tácito, desde que prestado de forma inequívoca, haverá, também, e não obstante, que ter em conta quer que o responsável por aquele deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais[15], quer o disposto a este propósito no *considerandum* 32 do RGPD. Pode ler-se aí que "o consentimento do titular dos dados deverá ser dado *mediante um ato positivo claro* que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser

[15] Releva a este ensejo a diferença entre as formalidades *ad probationem* e *ad substantiam*.

dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido". *Exclui-se expressamente* – e em consonância com a regra ditada pelo artigo 218º CC – *a relevância do silêncio como declaração de vontade, mas persistem dúvidas acerca do comportamento concludente como via de manifestação da vontade do sujeito*. Nada se estabelecendo a este respeito, valem, entre nós, numa interpretação sistemática dos preceitos do regulamento, as regras atinentes às declarações negociais, aplicáveis a esta questão ou diretamente ou por força do artigo 295º CC[16]. Parece, contudo, que, atentas as exigências probatórias e a necessidade de interpretar o corpo do regulamento à luz dos seus *considerandi*, pode ser defensável a exigência de uma declaração expressa, que não equivale, contudo, a uma declaração escrita. Atentemos, porém, nas orientações do grupo de trabalho do artigo 29º relativas ao consentimento na aceção do Regulamento (UE) 2016/679, nas quais se pode ler que "um «ato positivo inequívoco» significa que o titular dos dados deve agir deliberadamente para consentir o tratamento em causa". Assim, "a utilização de opções pré-assinaladas que o titular dos dados é obrigado a modificar para recusar o tratamento («consentimento baseado no silêncio») não constitui por si só um consentimento inequívoco"[17]. Mas considera-se que, "no âmbito dos requisitos do RGPD, os responsáveis pelo tratamento têm liberdade para desenvolver um fluxo de consentimento que se adeque às

[16] Sobre o ponto, cf., ainda, Paulo Mota PINTO, *Declaração tácita e comportamento concludente no negócio jurídico*, Almedina, Coimbra, 1995.

[17] Orientações do grupo de trabalho do artigo 29º relativas ao consentimento na aceção do Regulamento (UE) 2016/679, 18

respetivas organizações. A este respeito, as ações físicas podem ser consideradas um ato positivo inequívoco em conformidade com o RGPD".

No caso dos dados sensíveis – categorias especiais de dados previstos no artigo 9º RGPD – tem-se entendido que se deve exigir o consentimento explícito. De acordo com o grupo de trabalho do artigo 29º, "em termos jurídicos, entende-se que «consentimento explícito» tem o mesmo significado que «consentimento expresso». Abrange todas as situações em que as pessoas são confrontadas com a oportunidade de dar ou não o seu acordo para um uso especial ou divulgação da informação pessoal que lhes diz respeito e respondem ativamente a essa questão, verbalmente ou por escrito. Normalmente, o consentimento explícito ou expresso é dado por escrito, com a aposição de uma assinatura manuscrita. Por exemplo, é dado consentimento explícito quando a pessoa em causa assina uma autorização que estabelece claramente porque é que o responsável pelo tratamento pretende recolher e tratar os dados"[18].

[18] Parecer do grupo de trabalho do artigo 29º 15/2011, 29-30. Cf. Orientações do grupo de trabalho do artigo 29º relativas ao consentimento na aceção do Regulamento (UE) 2016/679, 20 s.: a referida declaração escrita não é a única maneira de obter consentimento explícito e não se pode dizer que o RGPD recomenda declarações escritas e assinadas em todas as circunstâncias que exigem um consentimento explícito válido. Por exemplo, num contexto digital ou em linha, o titular de dados pode emitir a declaração necessária preenchendo um formulário eletrónico, enviando uma mensagem de correio eletrónico, carregando um documento digitalizado com a assinatura do titular dos dados ou utilizando uma assinatura eletrónica. Em teoria, a utilização de declarações orais também pode ser suficiente para obter um consentimento explícito válido. Contudo, pode ser difícil para o responsável pelo tratamento provar que todas as condições aplicáveis

No contexto da massificação do uso de plataformas de *streaming*, colocam-se, desde logo, problemas no que respeita ao modo como o consentimento é obtido. Na verdade, v.g., se A se limita a aceitar um convite para participar numa reunião *zoom*, entra diretamente na plataforma, sem necessidade de subscrever qualquer serviço, mas sujeitando-se à recolha de dados pessoais para finalidades que desconhece por completo, ainda que seja o próprio a ativar o vídeo e o auscultador. Será isto bastante para garantir a licitude do tratamento de dados, quando o consentimento apenas é prestado em relação a certos dados?

Repare-se, neste contexto, que o consentimento tem de ser prestado *livremente*[19]. E que, para o ser, tem de ser *esclarecido*. Daí que o titular dos dados tenha direito à prestação de uma série de informações, por parte do responsável, que lhe permitam compreender a natureza e o alcance do ato, bem como acompanhar o tratamento que deles seja feito. O direito à informação de que se cura tem um âmbito e uma intencionalidade mais vastos do que de mero instrumento de esclarecimento conducente à licitude do

---

ao consentimento explícito válido foram satisfeitas quando a declaração foi gravada. Uma organização também pode obter consentimento explícito através de uma conversa telefónica, desde que as informações acerca da escolha sejam leais, inteligíveis e claras, e desde que a organização solicite uma confirmação específica ao titular dos dados (p. ex. pressionar uma tecla ou fornecer confirmação oral)".

[19] Cf. o artigo 7º/4 Regulamento, nos termos do qual "o avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato". *Infra,* teceremos esclarecimentos importantes sobre este preceito.

consentimento. Por um lado, ele continua a existir, quando o tratamento dos dados se baseie noutros fundamentos que não essa autorização do titular; por outro lado, ele revela-se essencial para que o titular dos dados pessoais possa acompanhar o tratamento que deles seja feito. Parece, aliás, ser esta a *ratio* do direito à informação a que se refere o artigo 15º RGPD e que surge associado ao direito de acesso do titular dos dados. Tal direito de acesso é subsequente à recolha dos dados. Por outro lado, a concretização do direito à informação, tal como acontecia no âmbito da lei nº67/98, vai ser diverso consoante os dados tenham sido recolhidos diretamente junto do seu titular ou não. É esta a solução que decorre dos artigos 13º e 14º RGPD.

Embora não confinado à necessidade de garantir a plena liberdade, o esclarecimento prévio ao consentimento para o tratamento de dados é condição imprescindível para que o mesmo possa ser considerado livre, e, como tal, válido. De outro modo, o titular dos dados não acederia à compreensão do âmbito e da dimensão do consentimento que estaria a prestar. A informação a que se alude deve ser simples, clara, compreensível por um titular de dados pessoais mediamente esclarecido[20]. Deve, além disso, ser completa e ser prestada antes de o consentimento ser dado, não bastando que esteja disponível num qualquer local[21]. Sublinhe-se que, quando o consentimento é prestado através de um formulário elaborado de forma prévia, unilateral e rígida por uma das partes, se devem aplicar as regras contidas no DL nº446/85, relativas aos contratos de adesão, donde os requisitos da comunicação e da

[20] Parecer do grupo de trabalho do artigo 29º 15/2011, 22
[21] Parecer do grupo de trabalho do artigo 29º 15/2011, 22

informação contidos nos artigos 5º e 6º do citado diploma se devem aplicar. Suscitam-se, portanto, dúvidas no que respeita à utilização que por vezes seja feita das plataformas de *streaming*: cumprir-se-á o dever de esclarecimento prévio a que se alude e que surge como garantida da validade do consentimento?

Mas, a natureza livre do consentimento levanta ainda outras questões relevantíssimas. O *considerandum* 43 do RGPD dispõe que, «a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa».

Significa isto que, em situações como as que envolvem a utilização de plataformas de teletrabalho, podemos confrontar-nos com um problema: na verdade, sendo o trabalhador forçado a executar a prestação de trabalho, dificilmente podemos considerar que o consentimento é livre. Alias, a doutrina costuma afirmar que poderá também não haver consentimento livre quando o titular dos dados se encontra numa situação de dependência (por exemplo, numa relação laboral). Ora, ainda que o consentimento não seja prestado diante da entidade patronal, mas perante um terceiro que gere a plataforma de *streaming* (o responsável pelo tratamento de dados

ou *controller*[22]), é percetível a falta de liberdade no comportamento do trabalhador[23]. Exclui-se a liberdade do consentimento sempre que haja uma situação de dependência, coação ou necessidade[24]. E este parece ser o caso das hipóteses em apreço, o que exige que se procure outro fundamento de legitimação do tratamento de dados[25].

---

[22] Discutiremos, *infra*, a qualidade da entidade patronal no quadro do tratamento de dados a que nos referimos.

[23] Parecer do grupo de trabalho do artigo 29º 15/2011, 19

[24] Orientações do grupo de trabalho do artigo 29º relativas ao consentimento na aceção do Regulamento (UE) 2016/679, adotadas em 28 de novembro de 2017 e revistas em 10 de abril de 2018. Considera-se, aí, que "o elemento «livre» implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido".

[25] A propósito do consentimento, importa, também, considerar que o Regulamento estabelece regras atinentes ao *consentimento por menores*. Dispõe o artigo 8º que "quando for aplicável o artigo 6º/1 a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança". A esta solução já seria possível chegar com base nas regras próprias do ordenamento jurídico português. Para tanto seria, no entanto, necessário perscrutar a natureza do direito à proteção de dados. Refira-se que os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos. De acordo com o artigo 16º da Lei nº58/2019, de 8 de agosto, "nos termos do artigo 8º do RGPD, os dados pessoais de crianças só podem ser objeto de tratamento com base no consentimento previsto na alínea a) do nº 1 do artigo 6º do RGPD e relativo à oferta direta de serviços da sociedade de informação quando as mesmas já tenham completado 13 anos de idade. Caso a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento

No quadro de uma utilização não pessoal e não voluntária das referidas plataformas, torna-se necessário encontrar outro fundamento para o tratamento de dados que não o consentimento. Há, então, que relembrar (uma vez mais) o artigo 6º/1 RGPD: o tratamento é lícito quando 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; quando seja necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; quando seja necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; quando seja necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; quando seja 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.

A realidade mostra-nos que, em muitas situações, pode não existir um contrato entre o titular dos dados e a plataforma de *streaming*, sendo a parte contratual a entidade patronal que organiza os meios de teletrabalho e os disponibiliza ao trabalhador, celebrando um

---

for dado pelos representantes legais desta, de preferência com recurso a meios de autenticação segura". Significa isto que o legislador português, usando a prerrogativa que é concedida aos diversos Estados membros pelo artigo 8º RGPD, fixou a idade mínima para prestar o consentimento nos 13 anos. Parece haver, desta forma, um desvio em matéria de capacidade no que respeita ao regime privatístico geral. Estes dados são particularmente relevantes se tivermos em conta que também os jovens em idade escolar, fruto do ensino à distância, se encontram forçados a utilizar as plataformas de *streaming*.

contrato com a entidade gestora da plataforma[26]. Então, a questão que se coloca é se podemos ver na defesa de interesses vitais do titular dos dados e das outras pessoas o fundamento específico de legitimação do tratamento que se faça. O que não deixa de ser, em si mesmo, problemático, porque – em rigor – essa não parece ser a finalidade do tratamento de dados que seja feita pela entidade gestora da plataforma. Dito de outro modo, assiste-se a uma triangulação (interesse vital dos titulares dos dados, que é salvaguardado pelo Estado e, mediatamente, pela entidade patronal; interesse específico no tratamento de dados da entidade gestora da plataforma; interesse do titular dos dados), que gera um desencontro entre uma finalidade legitimadora e a finalidade específica do tratamento em questão. A alternativa discursiva é vermos no contrato celebrado entre a entidade gestora da plataforma de *streaming* e a entidade patronal um contrato a favor de terceiros, nos termos dos artigos 443º e seguintes CC. Nessa hipótese, o fundamento de licitude do tratamento seria, ainda, a necessidade de execução de um contrato.

Mas, se assim for, o tratamento de dados deve orientar-se pela finalidade específica que o autoriza, o que implica que não seja possível proceder a um tratamento posterior de dados que vá para além do necessário para viabilizar a utilização da plataforma. Do mesmo modo, as obrigações enunciadas pela CNPD não podem deixar de ser cumpridas.

Assim, entre outros aspetos sublinhados pela CNPD, as

[26] O contrato com a plataforma é celebrado pela entidade patronal, que depois disponibiliza as credenciais de acesso aos trabalhadores.

plataformas escolhidas devem ter finalidades bem definidas; devem recolher e tratar os dados estritamente necessários para as finalidades especificadas; devem definir de forma clara os papéis e responsabilidades dos vários intervenientes no tratamento de dados pessoais, em especial a distribuição de funções e responsabilidades entre quem fornece e gere a plataforma e quem decide sobre a sua utilização; devem ser desenvolvidas de forma que os princípios de privacidade desde a conceção sejam aplicados, pelo que as configurações de privacidade devem estar predefinidas e a sua desativação ser da iniciativa do utilizador; devem comunicar aos utilizadores sempre que ocorrerem violações de dados pessoais; devem utilizar criteriosamente quaisquer algoritmos de análise de desempenho (*learning analytics*), que ficam ainda assim dependentes de expressa autorização do titular dos dados[27].

5. Alguns aspetos relativos à responsabilidade civil: violação de dados pessoais e possíveis responsáveis

Ao lidarmos com os problemas que a utilização de plataformas de *streaming* suscitam, confrontamo-nos com a hipótese de ocorrerem violações do direito à proteção de dados pessoais. *Quid iuris*, se efetivamente ocorrerem? Em abstrato, é possível que as referidas violações sejam perpetradas pelo responsável pela plataforma ou por um terceiro.

[27] Cf. CNPD, *Orientações para utilização de tecnologias de suporte ao ensino à distância*.

Vejamos, então.

5.1. A responsabilidade civil da entidade gestora da plataforma e/ou de um terceiro (*hacker*)

O regulamento europeu prevê, no artigo 82º, que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Acrescenta o nº2 do preceito que qualquer responsável pelo tratamento que nele esteja envolvido é responsável pelos danos causados por um tratamento que viole o presente regulamento, sendo o subcontratante responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações impostas pelo regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é responsável pelo evento que deu origem aos danos. Havendo mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, que sejam responsáveis por danos causados pelo tratamento, cada um é responsável pela totalidade dos danos, prevendo-se no nº5 do artigo 82º a possibilidade de exercício do direito de regresso em relação à parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com a regra estabelecida no nº2.

Por seu turno, o artigo 33º/1 Lei nº58/2019, de 8 de agosto, determina que "qualquer pessoa que tenha sofrido um dano devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições do RGPD ou da lei nacional em matéria de proteção de dados pessoais tem o direito de obter do responsável ou subcontratante a reparação pelo dano sofrido".

Torna-se, assim, inequívoco que o Regulamento 2016/679 consagra uma regra de solidariedade obrigacional entre os corresponsáveis, ao mesmo tempo que parece inverter o ónus da prova, a partir do momento em que se constata a violação das obrigações por ele impostas[28]. As soluções são de aplaudir, não só pelo cunho protetivo do titular dos dados que apresentam, como porque parecem resultar do funcionamento das regras ressarcitórias, quando entendidas numa ótica personalista. De facto, a partir do momento em que um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado – consagradas pelo legislador – no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (*responsabilidade pelo outro, ou pelos dados do outro*) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da *liability* (*responsabilidade perante o*

[28] A solução parecia já resultar da lei de proteção de dados nacional. O nº2 do artigo 34º prevê que "o responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano não lhe é imputável". A formulação legal peca, contudo, por não perceber que, se o evento não for imputável ao sujeito, não é possível afirmar-se a responsabilidade, não fazendo sentido falar de uma responsabilidade parcial. Teria, portanto, de se tratar de uma não imputação em termos também parciais, a obrigar a uma correção do preceito.

outro). A esta esfera são reconduzidos todos os danos-lesão que deveriam ser obviados pelo cumprimento do dever legal imposto, pelo que, *a priori*, cada interveniente no tratamento dos dados responderá pela totalidade do dano verificado em face do sujeito lesado. Posteriormente, pelo confronto entre a esfera de risco/responsabilidade do lesante e outras esferas de risco, aquele primitivo nexo imputacional que se desenha concretiza-se, podendo em concreto excluir-se ou conjugar-se com outros.

A responsabilidade pode, assim, ser assacada ao *controller* ou ao *processor*.

Nos termos do artigo 4º/7 RGPD, o responsável pelo tratamento (*controller* ou *controlador*) é "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

O responsável pelo tratamento de dados ou *controller* é, portanto, a pessoa, singular ou coletiva, que determina as finalidades e os meios de tratamento de dados, isto é, aquele que decide que meios são recolhidos e tratados, como e porque é que o são. No fundo, é a pessoa que exerce o controlo sobre os dados, razão pela qual lhe são impostos especiais deveres e lhe é imputada a responsabilidade, em caso de violação de algum deles. De acordo com a explicitação do Grupo de Trabalho do Artigo 29º sobre a Proteção de Dados, o

controlo de que aqui se fala pode resultar de três vias: de uma competência legal expressa; de uma competência tácita, no âmbito de uma relação contratual; ou de uma influência de facto[29]. Fundamental é que este controlo não seja meramente formal, pelo que, consoante se pode ler no documento europeu – embora por referência ao anterior quadro legislativo –, havendo nomeação legal do responsável pelos dados, ela deve refletir a realidade, devendo aquele que é indicado como *controller* exercer um controlo efetivo sobre os dados[30]. Do mesmo modo, nas outras vias de controlo, é essencial ter em conta as cláusulas de um eventual contrato, o grau de controlo efetivamente exercido, a imagem transmitida aos titulares dos dados, tendo sempre presente que releva mais o efetivo controlo material do que as eventuais classificações formais a que possamos ser conduzidos pelos negócios envolvidos na situação[31].

Se uma plataforma de *streaming* recolhe os dados dos seus clientes, quando com eles celebra um contrato de utilização daquela, havendo, depois, uma outra entidade que armazena, digitaliza e cataloga todas as informações relevantes, de acordo com as instruções específicas fornecidas pela primeira e para os fins que ela tenha estabelecido, então, a primeira é, neste contexto, o *controller*, ou seja, o responsável pelo tratamento dos dados. Mas, se a plataforma X contrata a empresa Y, que presta serviços de *marketing*

[29] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 14 s.
[30] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 14 s.
[31] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 16.

direto a várias empresas, para difundir os seus produtos junto dos seus clientes, e Y, para além de cumprir a obrigação a que está contratualmente vinculado, decide usar a base de dados que lhe foi transmitida pela entidade gestora da plataforma para promover, também, produtos de outros clientes, então, assume uma nova finalidade para o tratamento dos dados, passando a ser um *controller*, não obstante a eventual designação que possa surgir no contrato[32]. A solução é ditada pelo artigo 28º/10 RGPD, nos termos do qual "o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão", e vai ao encontro do que, por referência à anterior legislação europeia na matéria, era defendido pelo grupo de trabalho do artigo 29º para a proteção de dados. No parecer 1/2010, sobre os conceitos de responsável pelo tratamento e subcontratante, pode ler-se que "a determinação da finalidade de tratamento está reservada ao responsável pelo tratamento", pelo que quem assumir a decisão de eleger uma nova finalidade assume, igualmente, tal estatuto[33]. O raciocínio é, aliás, estendido pelo referido grupo de trabalho às pessoas singulares que se integram na estrutura organizacional do *controller*. Se, em regra, elas agem por conta da pessoa coletiva, não se distanciando dela, para efeitos de aplicação do regulamento, se, "ultrapassando o âmbito das atividades da

[32] A explicitação é feita pelo Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 18, que nos apresenta um caso com uma intencionalidade e uma estrutura problemáticas em tudo idênticas ao que aqui deixamos inscrito.

[33] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 19.

pessoa coletiva e escapando ao seu controlo, utilizar dados para os seus próprios fins", deve ser tratada como responsável pelo tratamento dos dados[34].

Não deixa, contudo, de ser estranha a perspetiva a que somos conduzidos por determinação legal, razão pela qual importa sobre ela tecer alguns esclarecimentos. Em primeiro lugar, resulta do exposto que a noção de *controller* é uma noção dinâmica, que não se deixa aprisionar por determinações abstratas formuladas *a priori*, antes procurando espelhar o efetivo controlo de facto sobre as finalidades e os meios de tratamento de dados. Por outro lado, ao dispor-se que o subcontratante que eleja uma finalidade nova e própria em relação aos dados que lhe foram transmitidos deve passar a ser tratado como responsável pelo tratamento de dados, pretende-se que, porque os dados passam a ser utilizados com outro objetivo e através de outros meios, independentemente da ilicitude que esta alteração já possa, em si mesma, comportar, as garantias de segurança que são oferecidas pelo regulamento ao titular dos dados se mantenham. Simplesmente, essa determinação só faz sentido quando a utilização dos dados segundo uma nova finalidade não tenha, por um lado, em vista uma violação dos direitos que subjazem à proteção de dados, e, por outro lado, quando a estrutura organizacional do sujeito que se convola em *controller* permita antever uma utilização dos dados em termos de efetivo controlo factual sobre eles e em termos de utilização consentânea com o regulamento, para lá da questão da ilegitimidade da utilização pela violação do consentimento. É que só nesses casos faz sentido impor

[34] Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 20.

ao novo *controller* as medidas protecionistas gizadas pelo legislador europeu. De outro modo, estar-se-ia a considerar que o que atua ilicitamente – e voltamos a frisar que a atuação ilícita existe sempre, pela utilização dos dados para uma finalidade não consentida – fica ainda vinculado, nessa sua atuação que o ordenamento jurídico repudia, por determinados deveres legais. No fundo, a única solução que se admite como sustentável – sem embargo da ilicitude de base com que nos possamos confrontamos – é a que, independentemente da responsabilidade que se possa desencadear, olha para uma utilização de dados que, se fosse consentida, não seria ilícita para lhe impor regras que a tornem efetivamente segura para os titulares daqueles dados. São, portanto, preocupações protecionistas que avultam maiores a este nível. Simplesmente, estas não são compagináveis com uma utilização que, independentemente da falta de consentimento, sempre se teria de reputar de ilícita porque violadora dos direitos que estão na base da proteção de dados. Pense-se, por exemplo, na hipótese de um sujeito que se aproveita da base de dados de um *controller* para eleger como nova finalidade (sua) do tratamento de dados a promoção de uma campanha atentatória da honra dos visados. É claro que, numa situação como esta, por maioria de razão, o sujeito em questão será responsável, mas sê-lo-á, não no sentido do controlo, mas no sentido da responsabilidade civil que avulta como remédio sancionatório. E para isso não necessitamos de o converter em *controller*, no quadro regulamentar, quer porque tal implicaria uma confusão entre duas aceções do termo responsável, quer porque o funcionamento das regras dogmáticas delituais (e, como veremos, contratuais) nos permite assacar essa mesma responsabilidade sem necessidade de atestar da violação das normas do regulamento.

Significa isto que a entidade gestora da plataforma de *streaming*, ao tratar os dados de que necessita para a execução do contrato ou outros que vai consentidamente recolhendo, aquando da utilização que dela se faça, deve ser visto como controller, podendo ser responsabilizada, nos termos do RGPD. Mas significa também que um *hacker* que viole dados pessoais não deverá ser responsabilizados nos termos do mesmo diploma. Aliás, em rigor, de acordo com o artigo 82º do citado diploma, a responsabilidade assimilada pelo seu âmbito de relevância reduz-se às hipóteses de violação das normas do regulamento por parte de um *controller* ou de um *processor*, o que não quer dizer que se afaste a responsabilidade do sujeito em questão. E se o âmbito de relevância do artigo 33º Lei nº58/2019, de 8 de agosto, parece ser mais amplo, ao admitir a responsabilidade do responsável ou do subcontratante, por um dano devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições do RGPD ou da lei nacional em matéria de proteção de dados pessoais, continua, contudo, a disciplinar unicamente a responsabilidade que se assaca ao *controller* ou ao *processor*, deixando de lado atos de terceiros que não assumam qualquer uma destas qualidades.

Donde, ou aceitamos que o terceiro/*hacker* pode ser visto como um *controller*, apesar da ilicitude de base do comportamento, e ele será responsável nos termos dos diplomas em apreço; ou recusamos tal possibilidade e a responsabilidade terá de ser disciplinada pelo Código Civil, seguindo os termos gerais.

Estas considerações não obstam, porém, a que a entidade gestora da plataforma seja responsável ainda que tenha havido a intervenção de um terceiro não autorizado. O artigo 82º/3 dispõe que "o responsável pelo tratamento (…) fica isento de responsabilidade nos

termos do nº2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos". O que o preceito estabelece é a regra da inversão do ónus da prova da imputação (outrora dita causalidade), de tal modo que, havendo mais do que uma esfera de responsabilidade em relação a um mesmo conjunto de dados, relativamente ao qual se verifica um evento danoso, ambos são responsabilizados solidariamente[35], exceto se, no posterior cotejo de esferas de responsabilidade a que se proceda, se perceba que a esfera de responsabilidade de um agente consome a do outro. Se deve ser assim em geral, há que sublinhar que geralmente a esfera de responsabilidade avulta unicamente a partir da constatação de um aumento do risco, ou seja, da preterição de deveres no tráfego. A especificidade que o Regulamento nos traz é, mais do que permitir que, uma vez violada uma regra por ele imposta, se presuma que a sua preterição foi culposa, considerar que o *controller* será sempre responsável pela violação dos dados, bastando que para tal esteja envolvido naquele tratamento. Ora, pode acontecer que o *controller* – a entidade gestora da plataforma –, embora não protagonize a violação do direito à proteção de dados (bem como a violação de outros direitos que lhe subjazem), viole determinados deveres a que estava adstrita enquanto responsável pelo tratamento de dados em questão, potenciando a intromissão de terceiros. Nessa medida, a responsabilidade entre ambos será solidária, tanto quanto não se consiga provar a falta de intervenção no tratamento de dados em causa.

Repare-se que esta responsabilidade pode também avultar no âmbito contratual. Em primeiro lugar, pode existir entre a plataforma

[35] A solidariedade resulta da conjugação entre o artigo 82º/3 e o artigo 82º/4 CC.

de *streaming* e o utilizador um contrato – são os *casos de utilização voluntária da plataforma*; noutras situações, o contrato é celebrado entre a entidade gestora da plataforma e a entidade patronal, podendo configurar-se um contrato a favor de terceiros – são os *casos de utilização não voluntária da plataforma*. E quer o tratamento de dados seja legitimado pela necessidade de executar o contrato, quer ele se baseie no consentimento, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram a referida responsabilidade contratual. A violação de deveres de conduta, porque reconduzidos ao núcleo da relação contratual, vista como uma relação obrigacional complexa, gera uma hipótese que é assimilada pela responsabilidade contratual.

5.2. A responsabilidade da entidade patronal que impõe o teletrabalho

Problema mais complexo, a este nível, é o que se prende com a eventual responsabilidade da entidade empregadora que impôs, no quadro do teletrabalho, a utilização de plataformas de *streaming*[36].

São cogitáveis diversas hipóteses. Num primeiro cenário, a entidade patronal desenvolve a plataforma de teletrabalho, com base nos seus próprios gabinetes informáticos, e fornece-a aos seus

[36] Ainda que a relação contratual seja firmada entre a entidade patronal e a plataforma de *streaming*, poderá haver responsabilidade contratual da segunda em relação ao trabalhador lesado, por se considerar que estamos diante de um contrato com eficácia de proteção para terceiros.

trabalhadores. Neste caso, a entidade patronal e a entidade gestora de teletrabalho coincidem, e aquela é tida como *controller*, podendo ser responsabilizada nos termos explicitados, quer de acordo com o RGPD, quer de acordo com as regras contratuais.

Num segundo cenário, a entidade patronal recolhe os dados dos seus trabalhadores, fornecendo-os à plataforma de *streaming*, que ou os trata de acordo com os meios e as finalidades definidas pela primeira, sendo, neste caso, a entidade patronal *controller*, e a entidade gestora da plataforma um *processor*; ou os trata de acordo com as suas próprias finalidades e meios, sendo também *controller*. Não cremos, porém, que a primeira sub-hipótese deste cenário corresponda muito frequentemente aos dados da realidade: o subcontratante (*processor)* é aquele que procede ao tratamento de dados por conta do *controller*. A atuação por conta de outro sujeito determina que as finalidades do tratamento não possam ser definidas pelo *processor*. Ora, ainda que a entidade patronal possa fornecer os dados dos seus trabalhadores, no quadro do contrato que celebra com a entidade gestora da plataforma (visto como um contrato a favor de terceiro), dificilmente será pensável que a finalidade do tratamento seja exclusivamente definida pelo empregador.

Num terceiro cenário, aquele que corresponde mais aos dados fácticos no nosso ordenamento, a entidade patronal apenas indica que as reuniões ou outros serviços são realizados numa dada plataforma de *streaming*, que define os próprios meios e finalidades do tratamento dos dados que recolhe para o cumprimento das suas obrigações. Entre a entidade patronal e a entidade gestora da plataforma é celebrado um contrato, que permite que os trabalhadores usem os serviços da segunda.

Nos dois primeiros cenários, a entidade patronal assume-se como *controller*. Na segunda hipótese do segundo cenário, avultam dois responsáveis pelo tratamento, o que não quer dizer que haja controlo conjunto. Para que haja controlo conjunto e, portanto, para que possamos falar de co-controladores (corresponsáveis), torna-se mister que haja efetiva partilha das finalidades e dos meios. Sempre que falhe esta conjunção, falha, também, a qualificação que se procura. O controlo conjunto a que se alude pressupõe, portanto, um domínio de facto comum dos dados, o que significa que a conjunção a que se alude envolve a possibilidade de ambas as entidades cumprirem as obrigações que o regulamento prevê. No fundo, para se falar de controlo conjunto, haveremos de estar diante de uma hipótese em que os mesmos dados são partilhados por mais do que uma entidade, unidas pela prossecução de uma finalidade comum ou pela utilização de meios definidos em conjunto, de tal modo que só conseguimos antever uma atividade de tratamento de dados[37]. O controlo conjunto não se confunde, portanto, com um

[37] Cf. Grupo de trabalho do artigo 29º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 27, colocando a questão de saber se o controlo conjunto envolve sempre a responsabilidade solidária e respondendo negativamente, por considerar que os diferentes responsáveis poderão ser responsáveis pelo tratamento de dados pessoais em fases diferentes e em diferentes graus. Não cremos, porém, que a posição do grupo de trabalho possa ser sufragada, mesmo descontando o facto de ela se reportar à anterior legislação comunitária na matéria. Em primeiro lugar, havendo mais do que um responsável no âmbito delitual, a regra é a da solidariedade, independentemente do grau de responsabilidade de cada um, que apenas se torna relevante no quadro das relações internas; em segundo lugar, ainda que a atuação de dois sujeitos não seja simultânea, a decisão de tratamento dos dados com base na finalidade eleita e nos meios escolhidos implica que há

controlo comum de certos dados que não envolva partilha de finalidades e de meios (e, portanto, que não envolva uma única atividade de tratamento de dados).

O controlo pode, portanto, ser conjunto ou paralelo, simultâneo ou sucessivo.

Havendo violação do direito à proteção de dados no quadro do tratamento conjunto que deles seja feito, avultará necessariamente a responsabilidade quer da entidade gestora da plataforma, quer da entidade patronal, em termos de solidariedade. Esta solução resulta dos artigos 82º/2 e 4 RGPD, estando em sintonia com o disposto no artigo 497º CC. É que o controlo conjunto a que se alude não mais representa do que uma estrutura problemática que, pela partilha de finalidade e de meios, determina que haja apenas um tratamento para o qual convergem duas esferas de responsabilidade subjetivas. Se aquele tratamento envolve a preterição de dados pessoais, então, porque o controlo de finalidades e meios é comum e determina um só tratamento, tornam-se atuantes diversas esferas de risco/responsabilidade. Simplesmente, a realidade fáctica parece afastar esta possibilidade.

No caso do controlo paralelo, se a violação dos dados ocorre no tratamento que é feito pela empresa de *streaming*, então, parece que apenas esta será responsabilizada pelos danos que possam

apenas uma atividade de tratamento de dados, embora titulada por mais do que um sujeito, e portanto reconduzível – na convolação da responsabilidade enquanto controlabilidade para a responsabilidade no sentido da *liability* – a mais do que uma esfera de responsabilidade. O controlo conjunto é incompatível com uma ideia de não solidariedade.

emergir.

Há que ter, no entanto, em conta alguns dados. Em primeiro lugar, a noção de tratamento de dados com que somos confrontados pelo regulamento é muito ampla. Nos termos do regulamento, o tratamento de dados é visto como uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. Significa isto que a simples transmissão dos dados para uma outra empresa integra o conceito de tratamento. Se o primeiro *controller* não se assegura da fiabilidade do cumprimento do regulamento por parte do segundo *controller* poderá ser por isso responsabilizado. É claro que, sendo o regulamento imperativo para todos os agentes, se poderá chamar à colação uma ideia de confiança para afastar, a este nível, a responsabilidade do primeiro. Simplesmente, nada exclui a possibilidade de a empresa de *gestão da plataforma de streaming* estar sediada fora da União Europeia. Ora, de acordo com o Regulamento, as transferências para países terceiros (bem como para organizações internacionais) só podem ser efetuadas no pleno respeito pelo presente regulamento, ou seja, só podem ter lugar se houver garantias de cumprimento de um nível de proteção idêntico ao que o regulamento dispõe por esse novo *controller*, o que significa que, apesar de o ato diretamente violador dos dados ser perpetrado pelo último, é possível que se venha a imputar ao primeiro também a responsabilidade, operando as regras da solidariedade, nos termos

do artigo 82º/4 RGPD.

Por outro lado, há que ter em conta que o artigo 82º/3 dispõe que "o responsável pelo tratamento (…) fica isento de responsabilidade nos termos do nº2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos". O que o preceito estabelece é a regra da inversão do ónus da prova da imputação (outrora dita causalidade), de tal modo que, havendo mais do que uma esfera de responsabilidade em relação a um mesmo conjunto de dados, relativamente ao qual se verifica um evento danoso, ambos são responsabilizados solidariamente[38], exceto se, no posterior cotejo de esferas de responsabilidade a que se processe, se perceba que a esfera de responsabilidade de um agente consome a do outro. Se deve ser assim em geral, há que sublinhar que geralmente a esfera de responsabilidade avulta unicamente a partir da constatação de um aumento do risco, ou seja, da preterição de deveres no tráfego. A especificidade que o RGPD nos traz é, mais do que permitir que, uma vez violada uma regra por ele imposta, se presuma que a sua preterição foi culposa, considerar que o *controller* será sempre responsável pela violação dos dados, bastando que para tal esteja envolvido naquele tratamento. Se é certo que, na hipótese em análise (de violação dos dados pela plataforma de *streaming*) tal não ocorre, porque o tratamento gerador da lesão é subsequente, ao considerarmos que a mera transferência de dados configura, em si mesma, um tratamento, haveremos de ter em conta que lhe cabe a si provar que não houve qualquer preterição das regras impostas em matéria de transmissão de dados. Repare-se, porém, que em muitas situações do que se trata é da lesão de dados pessoais que são

[38] A solidariedade resulta da conjugação entre o artigo 82º/3 e o artigo 82º/4 CC.

gerados no quadro da própria utilização da plataforma.

Outras hipóteses têm que ser, ainda, consideradas ao nível do controlo paralelo. Teremos de ver, na verdade, se entre a entidade patronal e a entidade gestora da plataforma se pode ou não discernir uma relação de comissão, que eventualmente pudesse fazer avultar a responsabilidade da primeira nos termos do artigo 500º CC. Contudo, sendo certo que a relação de comissão implica que a subordinação, dificilmente ela se poderá discernir no caso concreto. Se é certo que em abstrato a hipótese é configurável, não parece razoável, em face do circunstancialismo de base, considerar que haja a dita subordinação, atenta a especialização do serviço prestado pela plataforma.

Por outro lado, estando em causa relações contratuais, teremos de ter em conta o artigo 800º CC.

O primeiro *controller* responde, como se de um ato seu se tratasse, por todos os comportamentos lesivos levados a cabo por terceiros de que se sirva para cumprimento das suas obrigações. O desenho estrutural do artigo 800º CC é, então, absolutamente díspar, quando comparado com o do artigo 500º CC. Desaparece, a este nível, a dupla imputação para se fazer responder o devedor pelos atos dos auxiliares que utilize no cumprimento da obrigação como se fossem os seus próprios atos. Como sublinha Carneiro da Frada, "a técnica da lei é distinta. O que ela faz é projetar logo a conduta do auxiliar na pessoa do devedor para verificar se desse modo o devedor

incorreria ou não em responsabilidade"[39]. Trata-se do que o autor cunha por *teoria da ficção*, na medida em que "se ficciona o comportamento causador do dano na pessoa do devedor"[40], consubstanciando, de acordo com a lição de outros civilistas, uma verdadeira responsabilidade objetiva por ato alheio[41].Duas são as situações com que podemos ser confrontados: a) o devedor atua com culpa *in elegendo*, *in instruendo* ou *in vigilando*, devendo ser responsabilizado com base em culpa, para o que não seria necessário

[39] M. Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", *Direito e Justiça*, vol. XII, tomo I, 1998, 301.

[40] M. Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 302; Id., *Contrato e deveres de protecção,* Separata do Boletim da Faculdade de Direito da Universidade de Coimbra, Coimbra, 1994, 210. Em sentido próximo, cf., ainda, Menezes CORDEIRO, *Da responsabilidade civil dos administradores* das sociedades comerciais, Lex, Lisboa, 1997, 487

[41] Cf. Antunes VARELA, *Das obrigações em geral*, vol. II, 7ª edição (reimpressão), Almedina, Coimbra, 2001, 103. De acordo com Carneiro da Frada, não estaria em causa uma verdadeira responsabilidade objetiva. Segundo se pode ler no estudo citado do autor, "outro poderia ter sido o caminho do legislador. Em vez da descrita ficção, uma similar amplitude de responsabilidade teria sido obtida se se tivesse abertamente consignado uma responsabilidade objetiva pela utilização de terceiros no cumprimento do programa obrigacional. Se bem se reparar, sem ter então que «representar» uma responsabilidade por facto ilícito-culposo do devedor" – M. Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303. Cf., também, M. Carneiro da FRADA, *Contrato e deveres de protecção,* 209 s.
Aderindo à chamada teoria da ficção, cf. Maria da Graça TRIGO, *Responsabilidade civil delitual,* 249 s.

mobilizar o artigo 800º CC[42]; b) o devedor não atua negligentemente, mas ocorre um dano por virtude da atuação do terceiro auxiliar, e ele continua a ser responsabilizado, *ex via* artigo 800º CC[43]. O que divide a doutrina, a este ensejo, é saber se esta é uma responsabilidade objetiva por ato de terceiro ou uma direta responsabilidade do devedor. Enquanto alguns autores olham para o artigo 800º no sentido de o preceito consagrar uma pura responsabilidade objetiva; outros entendem que as situações em que há culpa *in vigilando, in instruendo* ou *in elegendo* da parte do devedor também são assimiladas pela sua intencionalidade prático-normativa. Daqui resulta, em termos de construção dos pressupostos de relevância do preceito, uma consequência importante. Assim, enquanto a maioria dos autores sustenta que a falta de culpa do auxiliar afasta a responsabilidade do devedor[44], outros como Carneiro da Frada

---

[42] Para a consideração de ordenamentos jurídicos onde se chega à solução da responsabilidade contratual por facto de outrem sem que haja um preceito análogo ao artigo 800º CC, cf. René RODIÈRE, "Y a-t-il une responsabilité contractuelle du fait d'autrui?", *Recueil Dalloz*, Chr., 1952, 18 s.

[43] Veja-se, num sentido próximo, Ernst von CAEMMERER, "Verschulden von Erfüllungsgehilfen", *Festschrift für Fritz Hauß*, Karlsruhe, 1978, 38 s. Para o autor, o devedor poderá ser responsável por culpa *in elegendo*, naquelas situações em que escolhe incorretamente o seu auxiliar (v.g., escolhe uma pessoa que não tem as competências devidas ou é inimputável); caso o seu comportamento não seja culposo, então poderá continuar a ser responsabilizado, por via do §278 BGB, desde que o terceiro auxiliar atue com culpa. A falta de culpa do auxiliar determina a exoneração da responsabilidade do devedor, já que a missão do §278 não é ampliar a responsabilidade do devedor, mas torná-lo responsável como se tivesse sido ele próprio a atuar.

[44] Cf. Vaz SERRA, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", *Boletim do Ministério da Justiça*, nº72,

parecem depor em sentido contrário[45]. Importa ponderar o problema em função da intencionalidade normativa do preceito[46].

Em face de uma obrigação, em regra, o devedor não tem o poder de recusar uma prestação efetuada por um terceiro[47]. Por outro lado, aquele que está por ela vinculado até ao momento do cumprimento integral da prestação é sempre o devedor. O risco do não cumprimento da obrigação corre, por isso, por conta dele[48]. De

---

1958, 280 s.; Pessoa JORGE, *Ensaio sobre os pressupostos da responsabilidade civil*, Almedina, Coimbra, 1999 143 s.

[45] M. Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303. Para um aprofundado debate sobre a questão, cf. Maria da Graça TRIGO, *Responsabilidade civil delitual,* 247 s.

[46] Para além da chamada teoria da ficção, Carneiro da Frada indica outros tópicos para a fundamentação da responsabilidade do devedor pelos atos dos auxiliares: "se a utilização de auxiliares pelo devedor aumenta o seu raio de ação, potenciando os seus lucros, é também de elementar justiça que sobre ele recaiam os riscos correspondentes à sua atividade. É o devedor, aliás, quem os pode controlar melhor e, em qualquer caso, absorve-los com maior facilidade. Por isso também, como correspetivo desse risco da sua atividade, se compreende que ao credor esteja vedado interferir no programa de realização da prestação elaborado pelo devedor" – M. Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303.

[47] Cf. artigos 767º e 768º CC, para fundamentar a afirmação, bem como para evidenciar as situações em que o credor pode opor-se à realização da prestação por um terceiro.

[48] Veja-se, porém, *supra* a questão de saber se se deve ou não exigir a culpa do devedor, que se presumiria nos termos do artigo 799º CC. Sobre o ponto, cf. Karl LARENZ, *Lehrbuch des Schuldrechts*, I, *Allgemeine Teil*, München, 1979, 292 s. No ordenamento jurídico alemão, cf., ainda, Berthold KUPISCH, "Die Haftung für Erfüllungsgehilfen (§278)", *JuS*, 1983, 817 s.

acordo com o ensinamento de Vaz Serra, "o devedor responde por todos aqueles que deixou penetrar no seu domínio de atividade ou que admitiu a colaborar consigo de maneira mais ou menos permanente ou mais ou menos completa na execução das suas obrigações"[49]. Entende-se que assim seja. Na verdade, se o devedor não fosse chamado a responder independentemente de culpa própria, ele encontraria um expediente simples para excluir a sua responsabilidade. Bastaria, para tanto, que chamasse um terceiro para efetuar a prestação, o que, inclusivamente, poderia abrir a porta a abusos evidentes[50]. No fundo, intervindo aqui uma ideia de confiança, o devedor responde independentemente de culpa sua pelos danos que ocorram. Simplesmente, não se verifica a dupla imputação a que somos conduzidos por via do artigo 500º CC. E não

---

V., ainda e novamente, Maria da Graça TRIGO, *Responsabilidade civil delitual,* 251 s., dando conta da posição de Oertmann, que preconizaria a *ficção de existência de uma obrigação própria do auxiliar*, pelo que a ilicitude e a culpa teriam de se referir a essa pessoa, donde o auxiliar teria de ser imputável e não poderia ocorrer, em relação a ele, qualquer causa de exclusão da culpa; e da ideia de *ficção de que não teria sido o auxiliar a atuar, mas sim o devedor*, pelo que a questão da culpa se apuraria determinando se uma atuação correspondente do próprio devedor seria ou não culposa. Assim, se o devedor, em caso de comportamento equivalente, fosse imputável e não se verificassem causas de exclusão da culpa, haveria responsabilidade.

[49] A. Vaz SERRA, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 273 s.

V., igualmente, Pessoa JORGE, *Ensaio*, 149, considerando que o artigo 800º vem impedir que o devedor invoque a inexecução da obrigação imputável ao auxiliar e determinar que ele continua sujeito à sua obrigação inicial e à correlativa responsabilidade.

[50] Cf. A. Pinto MONTEIRO, *Cláusulas limitativas e de exclusão da responsabilidade*, Almedina, Coimbra, 2003, 284 s.

se verifica porque o contrato que alicerça a responsabilidade define, *a priori*, o obrigado e, portanto, o responsável em caso de incumprimento (em sentido amplo). O que o artigo 800º vem esclarecer é que a imputação dos danos ao devedor não se perde pelo simples facto de ele ter utilizado um terceiro, seu auxiliar[51], no cumprimento da obrigação[52]. Nessa medida, ainda que objetivada, a

[51] Os autores têm sublinhado que estes auxiliares podem ser, indiferentemente e para efeitos da mobilização do regime do artigo 800º CC, auxiliares dependentes ou independentes. Nesse sentido, cf. Pinto MONTEIRO, *Cláusulas limitativas*, 287 s.; Menezes CORDEIRO, *Da responsabilidade civil dos administradores*, 487, n.61; Maria da Graça TRIGO, *Responsabilidade civil delitual*, 242 s.; Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", *Revista de Direito e Economia*, ano XV, 82 s.
A este propósito, *v.*, igualmente, o problema enunciado por Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", *Revista de Direito e Economia*, ano XV, 92: até que ponto se integra a atividade de um terceiro na previsão do artigo 800º/1 CC? Em causa está, por exemplo, a determinação da eventual responsabilidade do devedor pela atividade dos correios ou dos caminhos-de-ferro, que utiliza para enviar a coisa objeto da prestação ao credor. De acordo com o ensinamento da doutrina alemão, referida por Maria Victória Rocha, haveria exclusão da responsabilidade quando a atuação da empresa fosse monopolista. Mais esclarece que o §287 BGB não é fonte de imputação de novos deveres. Cremos que o caráter monopolista ou não da atuação do terceiro não é significativo para a resolução da questão concretamente considerada. Na verdade, a solução para o problema há-de passar aos nossos olhos pela determinação do âmbito da obrigação a que se vinculou o devedor. Só a análise desse âmbito será de molde, em harmonia com a ideia de que o §287 BGB não é fonte de novos deveres (e, portanto, com a ideia de que o artigo 800º CC não é, também, fonte de novos deveres), a esclarecer o decidente no caso concreto.
[52] A este propósito, cf. Hugo NATOLI, L'attuatione del rapporto obbligatorio (appunti delle lesioni), tomo II, 2ª ed., Milano, 1967, 96-99, *apud* Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 80 s. O autor considera que

responsabilidade há de configurar-se como uma responsabilidade direta do devedor[53-54]. Em rigor, aliás, a ideia de controlo da atuação

não se deve falar, em rigor, de uma responsabilidade objetiva, por se exigir a culpa do auxiliar. Apenas sucede que o facto do terceiro é imputável ao devedor como *causa causae*, o que afeta não a culpa, mas o nexo causal.
Refira-se, porém, que o nosso entendimento olha para o problema do ponto de vista da imputação e não do ponto de vista da causalidade.

[53] Para um elenco das possíveis justificações que vão sendo avançadas para a solução contida no artigo 800º CC, cf. Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 81: necessidades práticas económico-sociais que se manifestam na necessidade de responderem pelos riscos da atividade aqueles que dela tiram proveitos; garantia contra a eventual insolvência dos auxiliares; extraneidade do credor relativamente à escolha dos auxiliares; presunção de culpa *in viligando* ou *in elegendo*; poder de prevenção do perigo; exigência de uma garantia tacitamente prestada pelo devedor ao credor.
Para um elenco de outros possíveis fundamentos, cf. Pedro MÚRIAS, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 208 s.: ideia de confiança; ideia de responsabilidade pelo próprio círculo de vida; benefício que o devedor terá ao alargar as suas possibilidades de ação (e, assim, de lucro); necessidade funcional do tráfico negocial. O autor mostra-se crítico de todas estas justificações.
V., igualmente, Ernst von CAEMMERER, "Verschulden von Erfüllungsgehilfen", 39 s.; Karl LARENZ, *Lehrbuch des Schuldrechts*, 297 s.

[54] Cf., num sentido próximo, Pedro MÚRIAS, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", *Revista da Faculdade de Direito da Universidade de Lisboa*, vol. 37, nº1, 1996, 211. O autor considera que a lei estabelece inúmeras limitações ao devedor que pretenda exonerar-se dos seus deveres ou fazer perigar os fins de alguns deles através da intervenção de terceiros e considera que nesse grupo de normas se integra o artigo 800º CC. No fundo, o fundamento do artigo 800º passa nela tutela do credor, que não se vê assim privado de garantias por ato livre do titular do dever. Para o autor, não será, portanto, necessário recorrer a outra ordem de razões. O artigo "colhe a sua plena fundamentação na existência de um qualquer dever e na necessidade

do auxiliar pelo devedor como justificativa da disciplina normativa contida no artigo 800º CC, aproximando a solução da plasmada no artigo 500º CC, perde-se por completo se tivermos em conta os representantes legais, por cujos atos também responde o património do devedor[55]. Aproximamo-nos, assim, dos autores que sublinham que a intencionalidade do preceito não é alargar o âmbito da responsabilidade do devedor, fazendo-o assumir o risco de utilização de auxiliares. Na verdade, do que se trata é de fazer o devedor responder como se fosse ele próprio a atuar[56]. A intencionalidade normativa que foi encontrada para o artigo 800º CC –

---

sentida pelo ordenamento de assegurar a obtenção das finalidades prosseguidas pela atribuição desse dever perante a introdução de um terceiro no âmbito do seu cumprimento". Como veremos o autor extrai, a partir deste fundamento, conclusões que não subscrevemos. Por outro lado, em vez de se cingir aos deveres de tipo obrigacional, aloja no âmbito de relevância do preceito qualquer dever. Estes os dois pontos de dissenso em relação a Pedro Múrias, que a seu tempo densificaremos.

[55] Repare-se que Maria Victória Rocha explicita que, no tocante à responsabilidade do devedor pelos atos dos representantes legais, se os efeitos da atuação destes se projetam na esfera do incapaz, é justo que seja o património dele a suportar as consequências dessa atuação. *V.* Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 79, n. 131.

Sobre a questão dos representantes legais, cf. Kurt BALLERSTEDT, "Zur Haftung für Culpa in contrahendo bei Geschäftsab-schluβ durch Stellvertreter", *Archiv für die civilistische Praxis*, 151, 1950/1, 501 s.

[56] Cf. Ernst von CAEMMERER, "Verschulden von Erfüllungsgehilfen", 39.

V., igualmente, Vaz SERRA, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 269 s.

Para outros desenvolvimentos, cf. Mafalda Miranda Barbosa, "Acerca da aplicação do artigo 800º CC aos ilícitos extracontratuais – breve apontamento", *O direito*, ano 147º-III, 2015

responsabilização direta do devedor, por ser ele o obrigado perante o credor, tratando-se o ato do auxiliar como um ato dele próprio – tem consequências ao nível da definição dos pressupostos de mobilização do regime.

Os autores costumam, a este propósito, apontar quatro requisitos para a procedência de uma pretensão indemnizatória fundada no artigo 800º CC: a existência de uma obrigação; a relação entre o devedor e o terceiro utilizado no cumprimento; a atuação do terceiro no cumprimento[57]; e a atuação do auxiliar[58].

Ora, qualquer um destes pressupostos tem de ser densificado à luz do recorte intencional anteriormente desenhado. Por isso, embora a lei não indique expressamente que a atuação do auxiliar tem de ocorrer no cumprimento da obrigação, a doutrina tem reforçado tal entendimento, afirmando que o devedor apenas é

---

[57] Segundo a maioria da doutrina, não se aplica, então, o artigo 800º nos casos em que não está em causa o auxílio ao cumprimento, ou seja, nos casos em que os danos foram causados por terceiros a quem o devedor facultou o uso ou gozo da coisa pertencente ao credor. Neste caso, aplicar-se-ia o artigo 1044º CC. Cf. Antunes VARELA, *Das obrigações*, II, 103, n.2; M. Carneiro da FRADA, *Contrato*, 217. Em sentido contrário, Pedro MÚRIAS, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 206, considerando que o artigo 1044º é uma concretização do artigo 800º CC.
Note-se que, nestas situações, estar-se-á, de facto, diante de uma hipótese de responsabilidade contratual. Basta pensar que entre os deveres de proteção resultantes do contrato, por via da boa-fé, se inscreva o dever de salvaguarda da propriedade alheia. A aplicação ou não do artigo 1044º para além das hipóteses de locação ficará dependente de se poder ou não reconduzir a lesão verificada ao núcleo de relevância obrigacional.

[58] Cf. Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 83 s.; Maria da Graça TRIGO, *Responsabilidade civil delitual*, 241 s.

responsável pelos atos praticados no cumprimento das obrigações e não pelos atos praticados por ocasião do cumprimento ou com relação indireta com o mesmo[59]. Estamos em crer, no entanto, que não podemos estabelecer, aqui, o paralelo com os problemas patenteados pelo artigo 500º CC. Na verdade, se diante da necessidade de densificar o conceito de *exercício das funções*, o jurista se confronta com dificuldades imputacionais evidentes, ao nível do artigo 800º CC somos desonerados da tarefa na medida em que a responsabilidade é balizada, *a priori*, pelos deveres que entretecem a relação obrigacional. Por isso, o nódulo problemático agigantar-se-á não diante da violação dos deveres de prestação, mas diante da violação dos deveres acessórios e dos deveres de

[59] Maria da Graça TRIGO, *Responsabilidade civil delitual*, 241 s.; Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 94; M. Carneiro da FRADA, *Contrato*, 251.

conduta[60-61]. Também o pressuposto da culpa deve ser compreendido

[60] De notar, porém, que a dificuldade ultrapassa o âmbito de relevância do artigo 800º CC. Na verdade, este problema surge paredes-meias com aquele outro que passa por saber se, mesmo quando a atuação é própria do devedor, a violação de deveres de conduta origina responsabilidade contratual ou não.
Sobre o ponto, cf. Carneiro da FRADA, *Contrato*, onde o autor defende a existência de uma terceira via de responsabilidade civil. Veja-se, também, Mafalda Miranda BARBOSA, "O problema da integração das lacunas contratuais à luz de considerações de carácter metodológico – algumas reflexões" e *Liberdade versus responsabilidade*, com uma posição diversa. Para outros desenvolvimentos, cf. Mafalda Miranda BARBOSA, *Lições de responsabilidade civil*, Princípia, 2017.
A este propósito, *v.*, igualmente, Carneiro da FRADA, *Contrato*, 154 s. e 169 s., considerando que o dano produzido por ocasião do cumprimento é um risco não típico e sensivelmente agravado pela entrada numa relação contratual. No fundo, embora o autor não reconduza todos os deveres de conduta à relação contratual, importa sublinhar que é ainda a economia negocial traçada pelas partes que permite solucionar o problema que temos em mãos.
[61] Sobre o ponto, cf. Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 93, considerando que a expressão *no cumprimento* deve ser entendida como abrangendo a relação obrigacional no sentido de relação obrigacional complexa. No tocante aos deveres acessórios de conduta, a autora esclarece que a jurisprudência alemã parte do critério da existência ou não de uma conexão íntima entre a atividade danosa e a tarefa de que o auxiliar foi encarregado pelo devedor, tornando-se, por isso, necessário que haja uma interferência do terceiro nos bens do credor em virtude da especial relação de confiança entre credor e devedor. A autora acaba por fazer apelo a uma ideia de causalidade adequada a este nível.
Duas notas se impõem a este ensejo.
Em primeiro lugar, chamamos a atenção para a improcedência do critério da causalidade adequada, em geral, e em particular. Em segundo lugar, importa esclarecer que o sentido imputacional que se procura delinear há-de ser encontrado por referência à obrigação que o devedor assumiu. No fundo, o exercício que se terá de levar a cabo passa por questionar se, atuando daquela

a esta luz. Se a responsabilidade do terceiro auxiliar é tida como responsabilidade do próprio devedor, então deve entender-se que, uma vez excluída a culpa do primeiro, se exclui concomitantemente

forma, o devedor seria ou não responsabilizado, por via da responsabilidade contratual.

Sobre o ponto, cf., ainda, Pedro MÚRIAS, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 204 s. O autor considera que devemos questionar, no tocante aos casos em que existe a violação de deveres de proteção, por ocasião do cumprimento, "se tivesse o ato sido praticado pelo devedor, ele responderia obrigacionalmente? Se sim, responde também agora pelo seu auxiliar. E não se diga que assim dispara o risco de responsabilidade para o devedor (…). O critério, seguido pela doutrina maioritária, dos *interesses ligados à relação contratual*, para determinar o quadro dos atos do auxiliar por que o devedor responderia, iria excluir a responsabilidade do relojoeiro cujo aprendiz partisse um relógio, atirando-o, em fúria, à cabeça do seu mestre, quando é patente que sem a relação contratual nunca o aprendiz teria a possibilidade de tocar no relógio, quanto mais de parti-lo". Concordamos com a solução patenteada pelo autor. Divergimos, contudo, nas conclusões a que chega. Na verdade, Pedro Múrias, considerando não estar aqui a violação de um dever contratualmente assumido, entende que estamos diante de uma responsabilidade que se funda num dever genérico de respeito pelos direitos absolutos, razão bastante para o autor não conseguir, em termos normativo-intencionais, distanciar o artigo 800º, que aqui chama à colação, do artigo 500º CC. Dá, portanto, um passo em frente no sentido da defesa de uma posição monista em matéria de modalidades ressarcitórias. Pelo contrário, consideramos que o relojoeiro do exemplo de escola, ao assumir a obrigação principal de reparação do relógio, assume também o dever de guarda da coisa, pelo que responderá ao nível obrigacional pelo dano que ocorreu.

a responsabilidade do segundo[62-63].

Quer isto dizer – com o caráter necessariamente sincopado que estas considerações denotam – que será o âmbito da obrigação previamente assumida pelo devedor que demarcará o âmbito da responsabilidade do devedor por via do artigo 800º CC, pelo que se pode afirmar que imprescindível a este nível é que haja uma obrigação em sentido técnico, sem a qual, aliás, não existiria sequer um devedor. No fundo, a chamada à colação do regime da

---

[62] Neste sentido, cf. Antunes VARELA, *Das obrigações*, II, 103 s.
Ressalvam-se, contudo, as hipóteses em que o devedor agiu com culpa, na escolha do auxiliar.
Para outros entendimentos acerca do problema, *vide*, novamente, Carneiro da FRADA, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303; Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 97 s.; Maria da Graça TRIGO, *Responsabilidade civil delitual*, 246 s. (questionando, designadamente, como poderemos aferir a culpa do auxiliar se ele não está vinculado por nenhuma obrigação).

[63] Outros problemas são também abordados pela doutrina a este nível. Assim, por exemplo, tem-se colocado a questão de saber se podem ser equiparados aos auxiliares as máquinas, quando o erro em que incorrem não se traduza num erro de programação. Sobre o ponto, cf. Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 82 s.
Também se indaga em que medida a escolha do terceiro feita pelo credor pode ter consequências ao nível da exclusão da responsabilidade do devedor. Sobre o ponto, cf. Maria Victória ROCHA, "A imputação objectiva na responsabilidade contratual", 88 s. Sublinha a autora que, se o terceiro surge como um colaborador do credor, exclui-se a responsabilidade do devedor. O mesmo não sucederá se o terceiro for escolhido entre os colaboradores do devedor. *Vide*, igualmente, Vaz SERRA, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 267 s.

responsabilidade contratual, a este nível, só é possível quando a legitimação para o tratamento de dados pessoais seja negocial.

No terceiro cenário cogitado, a entidade patronal não é *controller*, isto é, não é responsável pelo tratamento de dados. Simplesmente, ao impor a "obrigação" de contratação com a plataforma ou de utilização da plataforma, acaba por não ser alheia à situação gerada. Várias possibilidades assomam no horizonte do jurista.

Em primeiro lugar, podemos continuar a pensar no contrato celebrado entre a entidade patronal e a plataforma de *streaming* como um contrato a favor de terceiro. Simplesmente, sendo, neste caso, devedor a referida entidade que gere a plataforma, não se poderia equacionar a responsabilidade do empregador por via contratual, por este fundamento.

Há, no entanto, outro contrato do qual não nos podemos esquecer: o contrato de trabalho. Nesse âmbito, a entidade patronal obriga-se a pagar a retribuição do trabalho ao seu empregado. Mas obriga-se a mais: obriga-se ao cumprimento de uma série de deveres acessórios e de deveres de conduta. Há, de facto, toda uma panóplia de deveres que devem ser cumpridos no sentido de garantir a segurança dos trabalhadores[64]. Designadamente, a entidade patronal obriga-se a proporcionar boas condições de trabalho, do ponto de vista físico e moral e a prevenir riscos. O surgimento de novos riscos associados ao mundo digital exige uma interpretação das normas em que tais deveres são impostos no sentido da integração no seu âmbito de relevância daqueles deveres de prevenção do perigo digital. Se tal não nos autoriza a uma extensão teleológica do regime

[64] Cf. artigo 127º C. Trabalho.

da responsabilidade por acidentes de trabalho, por o jurista se ver aí confrontado com um princípio de limitação da autónoma constituição normativa, no tocante ao âmbito das lesões ressarcíveis, sempre haveremos de aventar a possibilidade de se gerar responsabilidade contratual, por violação positiva do contrato, ou responsabilidade extracontratual, por lesão de direitos de personalidade, em relação aos quais a entidade empregadora se assumia como garante. A responsabilidade é aqui uma responsabilidade por facto próprio. Designadamente, poderá ser responsável pelo facto de o terceiro, por si escolhido, não oferecer garantidas de cumprimento dos deveres de cuidado a que está obrigado na salvaguarda da incolumidade do trabalhador. Na ponderação que houvesse de ser feita em concreto, haveríamos de ter em conta determinados aspetos. Em primeiro lugar, a entidade patronal haveria de garantir, com base em informações que pudesse recolher, que a plataforma de *streaming* aconselhada ou imposta cumpria os requisitos de segurança. Mas, a necessidade de garantir a continuação da prestação de trabalho, para salvaguarda dos próprios trabalhadores, poderia determinar que não houvesse exigibilidade de cumprir requisitos mais apertados de segurança. A responsabilidade poderia, também, ser afastada, ao nível da imputação objetiva, por força de uma ideia de diminuição do risco (se o que se quiser, efetivamente, é diminuir o risco de contágio do trabalhador). No fundo, em causa, poderia estar, por parte da entidade patronal, o cumprimento de deveres de segurança dos trabalhadores, procurando preservar a sua saúde e integridade física.

Mas, se o que está em causa é a preservação da saúde e da integridade física dos trabalhadores, então, a entidade gestora da plataforma de *streaming* pode surgir como um terceiro de que

aquela se serve para cumprimento dos seus deveres, no âmbito de uma relação complexa que é a relação laboral. Ora, se assim é, então, a entidade patronal irá responder pelos danos causados pelo terceiro que usa no cumprimento das suas obrigações.

Consoante explicita Maria Victória Rocha[65], a expressão *no cumprimento* deve ser entendida como abrangendo a relação obrigacional no sentido de relação obrigacional complexa. No tocante aos deveres acessórios de conduta, a autora esclarece que a jurisprudência alemã parte do critério da existência ou não de uma conexão íntima entre a atividade danosa e a tarefa de que o auxiliar foi encarregado pelo devedor, tornando-se, por isso, necessário que haja uma interferência do terceiro nos bens do credor em virtude da especial relação de confiança entre credor e devedor. Naquelas hipóteses em que foi celebrado um contrato entre a entidade patronal e a plataforma de *streaming*, não resta qualquer dúvida da possível responsabilização da primeira por via do artigo 800º CC. Mais duvidosa é a situação em que a plataforma de *streaming* não é incumbida de facultar os meios que, salvaguardando a vida e integridade física do trabalhador, garantam a prestação do trabalho, mas em que a entidade patronal se limita a aconselhar ou impor o uso de uma dada ferramenta ao seu empregado.[66].

Mafalda Miranda Barbosa

---

[65] Cf. nota 61.

[66] Repare-se, contudo, que isto não faz da entidade empregadora *controller* em relação aos dados pessoais. A responsabilidade afirma-se nos termos gerais e não nos termos do RGPD.

REVISTA DE
DIREITO COMERCIAL