Avaliação de conhecimentos a distância no ensino superior português: processos de monitorização e sua conformidade com o RGPD[1]

Saul A. N. Ferreira Leite[2]

Resumo: Os meios digitais eram já uma presença constante no quotidiano dos estudantes quando, em abril de 2020, a pandemia por COVID-19 lhe conferiu especial importância. As instituições de ensino superior socorreram-se dessa via para prosseguir com as atividades letivas em plena pandemia, abrindo portas à utilização de soluções para monitorização da avaliação a distância, que algumas acabariam efetivamente por adotar.

O presente estudo propõe-se a seguir uma proposta de classificação dessas soluções identificando, em cada caso, as suas funcionalidades, os dados pessoais tratados, os fundamentos de licitude admissíveis e a necessidade de realização de uma avaliação de impacto sobre a proteção dos dados (AIPD).

Palavras-chave: *RGPD, AIPD, monitorização eletrónica, avaliação a distância.*

Abstract: Digital communication used to be a constant presence in students' daily lives when, in April 2020, the COVID-19 pandemic gave it a particular important role. Higher education institutions started using

[1] **Declaração de princípio:** A presente reflexão resulta do trabalho desenvolvido em sede académica, sob orientação dos Professores Doutores Nuno David e Francisco Pereira Coutinho, não vinculando a posição institucional da CNPD – embora muito se agradeça todo o apoio e ensinamentos transmitidos pela Professora Doutora Filipa Urbano Calvão.

[2] Mestre em Engenharia de Telecomunicações e Informática pelo Iscte – Instituto Universitário de Lisboa. Consultor da Comissão Nacional de Proteção de Dados.

this means to continue the learning activities, opening the door to distance assessment monitoring solutions, which some have started to adopt.

This study intends to follow an already existent e-proctoring tools classification to identify, case by case, the functionalities, the processed personal data, the admissible lawfulness of processing and the need to carry out a data protection impact assessment (DPIA).

Keywords: *GDPR, DPIA, e-proctoring, remote assessment.*

1. Introdução

As aplicações informáticas que se propõem a monitorizar um processo de avaliação de conhecimentos a distância captaram, nos últimos anos e de forma tendencialmente global, a atenção dos estabelecimentos de ensino em geral e de ensino superior em particular.

Para tanto, muito contribuíram as restrições à circulação de pessoas e a suspensão das atividades de ensino e de avaliação presenciais, impostas pelos Estados um pouco por todo o mundo, aspirando conter a propagação da pandemia por COVID-19. Nesse contexto, as referidas medidas foram primeiramente aplicadas em Portugal no período decorrido entre 14 de março e 15 de maio de 2020[3], e mais tarde por declaração do estado de emergência e suas sucessivas renovações, que vigorou entre 9 de novembro de 2020 e 30 de abril de 2021[4]. As restrições acabariam ainda por se fazer sentir com a declaração do estado de calamidade[5] que vigorou entre 1 e 30 de maio de 2021.

[3] Início e fim determinados pela publicação do Decreto-Lei n.º 10-A/2020, de 13 de março, e do Decreto-Lei n.º 20-H/2020, de 14 de maio, respetivamente.

[4] Através da publicação do Decreto do Presidente da República n.º 51-U/2020, de 6 de novembro, e sucessivas renovações, cf. informação disponível em: <*https://www.parlamento.pt/Paginas/estado-emergencia.aspx*>.

[5] O estado de calamidade foi declarado através da publicação da Resolução do Conselho de Ministros n.º 45-C/2021, de 30 de abril, alterada pelas Resoluções do Conselho de Ministros n.ºs 46-C/2021, de 6 de maio, e 52-A/2021, de 11 de maio, tendo sido prolongado até 30 de maio, por publicação da Resolução do Conselho de Ministros n.º 59-B/2021, de 14 de maio.

O direito ao ensino – constitucionalmente previsto[6] – levou a que as instituições de ensino superior optassem pelos meios que garantissem a continuidade das atividades letivas, necessariamente a distância, equacionando alternativas ao tradicional regime de avaliação.

A colocação em prática de um regime de avaliação a distância sempre suscitaria questões do foro e, ainda, relativas à sua eficácia, mas também, relativamente ao processo de monitorização dos alunos, uma cuidada ponderação sobre o risco de ingerência nos seus direitos e liberdades fundamentais dos alunos, devido à sua monitorização

A este propósito, em abril de 2020, a Fundação para a Ciência e a Tecnologia (FCT), através da Unidade de Computação Científica (FCCN), iniciou junto da comunidade académica um projeto-piloto de sistemas de avaliação a distância – Piloto SAR[7] – para avaliar a experiência de utilização em ambiente de testes (provas de avaliação fictícias) relativamente a quatro soluções comerciais de monitorização a distância[8]. O projeto terminaria em julho do mesmo ano, concluindo[9] essencialmente que as soluções comerciais em geral, e particularmente as que foram testadas, não apresentavam àquela data o nível de qualidade e maturidade suficientes para a sua utilização em larga escala, nem respondiam às especificidades do sistema de ensino superior português. Num *webinar*[10] realizado a 22 de maio de 2020, organizado em parceria pela *MetaRed Portugal*[11] e a FCT, no qual intervieram, entre outros, os responsáveis universitários pela gestão das aplicações do Piloto SAR, destacou-se uma clara preocupação com o nível de intrusão de algumas das aplicações testadas, bem como a necessidade de conduzir uma

[6] Art.º 74.º da Constituição da República Portuguesa.

[7] Disponível em <*https://www.fccn.pt/noticias/fct-projeta-a-utilizacao-de-sistemas-de-avaliacao-remota-no-ensino-superior*>.

[8] Foram disponibilizadas as soluções '*ProctorExam', 'TestWe', 'Exam.net'* e '*Respondus'*, respetivamente geridas pela Universidade de Lisboa, Instituto Politécnico de Bragança, Universidade de Trás-os-Montes e Alto Douro e Universidade de Aveiro.

[9] RIBEIRO, Rui, CABRAL, Pedro e GOMES, João, "Relatório Final – Sistemas de Avaliação Remota", FCT, 2020.

[10] Disponível em: <*https://www.youtube.com/watch?v=FS4Ci_BwBUA*>.

[11] Associação de instituições públicas e privadas, de ensino superior.

adequada análise dos respetivos tratamentos de dados à luz do Regulamento Geral sobre a Proteção de Dados (RGPD).

Se o ótimo é inimigo do bom, a pressa é inimiga da perfeição, nos diria, mais não fosse, a sabedoria popular. Não obstante, no ano letivo seguinte, em que o ensino superior foi sobretudo caracterizado por um regime misto no qual as aulas decorriam simultaneamente em modo presencial[12] e a distância, algumas instituições de ensino superior portuguesas determinaram[13] a adoção de um regime de avaliação de conhecimentos a distância, em alguns casos obrigatório.

Não tardaria, contudo, à semelhança do que aconteceu noutros países[14], que os visados se insurgissem[15] contra a realização das provas através de específicos *softwares,* por entenderem estar em causa a violação do RGPD, da Lei n.º 58/2019, de 8 de agosto, e das orientações

---

[12] Por vigorarem exceções ao dever geral de recolhimento domiciliário e à proibição de circulação na via pública em concelhos de risco elevado, sempre que em causa estivessem deslocações às instituições de ensino superior.

[13] Por via da publicação do Despacho Reitoral n.º 8/2021, 21 de janeiro, (disponível em: <*https://gdoc.uevora.pt/695399*>), a Universidade de Évora determinou a suspensão imediata das atividades de avaliação presenciais e a adoção do modelo online, sempre que a tipologia das unidades curriculares/curso o permitisse. A decisão ocorreu após publicação do Comunicado do Conselho de Ministros de 21 de janeiro de 2021, que determinou a suspensão das atividades letivas e não letivas, a partir de 22 de janeiro e pelo período de 15 dias.

[O] Despacho n.º 21/2021, de 17 de março, da Diretora da Faculdade de Direito da Universidade de Lisboa, determinou que os exames escritos da época de recurso do 1.º semestre da licenciatura e do Mestrado em Direito e Prática Jurídica seriam realizados com recurso a meios de avaliação a distância e, se possível, com o apoio de um programa de controlo de realização das provas. Após contestação dos alunos, foi o mesmo posteriormente alterado pelo Despacho n.º 24/2021, de 25 de março.

[14] Em vários Estados dos Estados Unidos da América (EUA) ("Students are pushing back against proctoring surveillance apps", EFF, disponível em: <*https://www.eff.org/deeplinks/2020/09/students-are-pushing-back-against-proctoring-surveillance-apps*>), em França ("À l'université Paris 8, la télé surveillance des examens est jugée trop intrusive", Le Figaro, disponível em: <*https://etudiant.lefigaro.fr/article/a-l-universite-paris-8-la-tele-surveillance-des-examens-est-jugee-trop-intrusive_a0b940b4-811d-11ed-b9f4-d826a205a5b5*>), entre outros.

[15] (Em linha) Disponível em: <*https://www.jn.pt/nacional/software-usado-na-avaliacao--guarda-sons-e-imagens-de-universitarios-do-minho–13455740.html*>; e <*https://www.publico.pt/2021/03/25/p3/noticia/faculdade-direito-queria-gravar-movimento-som-exames-estudantes-contestaram-provas-voltam-presenciais-1955939*>.

da Comissão Nacional de proteção de Dados (CNPD)[16] relativas ao ensino a distância.

Nesta senda, viria a CNPD deliberar[17] sobre a utilização das aplicações *'Respondus'* (*'Lockdown Browser'* e *'Respondus Monitor'*), por uma universidade portuguesa, entendendo que no concreto caso o tratamento de dados era suscetível de violar os princípios da licitude, finalidade, da minimização dos dados e da proporcionalidade – art.º 5.º, n.º 1, alíneas *a), b)* e *c)*, do RGPD – e, ainda, que a empresa *Respondus, Inc*, recolhia amostras das gravações de áudio e vídeo para os seus próprios fins, sem que fosse obtido o consentimento dos alunos (p. 6). Concluiu, ainda, que os dados dos estudantes eram armazenados nos EUA, sem a adoção de medidas suplementares que permitissem garantir um nível de proteção essencialmente equivalente ao assegurado na União Europeia (p. 6v.).

Um pouco por toda a Europa verificaram-se episódios semelhantes, embora com desfechos variados.

Em setembro de 2021, também aquela Autoridade para a proteção de dados pessoais italiana, *Garante per la Protezione dei Dati Personali* (GPDP), aplicou à Universidade *Luigi Bocconi*, em Milão, uma coima no valor de 200.000 euros por entender que não estavam reunidas as condições de licitude para o tratamento de dados, nomeadamente de categorias especiais de dados, durante a utilização de um sistema para monitorização dos alunos. Na mesma deliberação[18] assinalou, ainda, a falta de informação aos titulares dos dados, a não observância da proteção dos dados desde a conceção e por defeito, a ausência de medidas apropriadas à mitigação

---

[16] Designadamente, das 'Orientações sobre a utilização de tecnologias de suporte ao ensino à distância' e 'Orientações sobre avaliação à distância nos estabelecimentos de ensino superior' (respetivamente disponíveis em: <*https://www.cnpd.pt/media/1encswse/orientacoes_tecnologias_de_suporte_ao_ensino_a_distancia.pdf*> e <*https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf*>).

[17] "Deliberação/2021/662", CNPD, disponível em: <*https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887*>.

[18] "Ordinanza ingiunzione nei confronti di Università Commerciale 'Luigi Bocconi' di Milano – 16 settembre 2021", GPDP, disponível em: <*https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988*>.

dos riscos e a violação do princípio geral das transferências (art.º 44.º, em consonância com os Considerandos n.º 101 e 102, do RGPD).

Num outro caso[19], na sequência das averiguações por si iniciadas, em 30 de abril de 2020, a Autoridade de Proteção de Dados dinamarquesa (*Datatilsynet*) decidiu a favor da Universidade de Tecnologias de Informação de Copenhaga (ITU), que se socorreu do *software ProctorExam* para monitorizar os alunos de uma certa unidade curricular[20], através de um processo de avaliação a distância. Entendeu a Autoridade que foi realizada uma avaliação correta e documentada da necessidade de recurso àquela solução, que gravou o áudio e vídeo de 330 examinandos, bem como o conteúdo dos seus monitores, revelando-se a menos intrusiva face às circunstâncias. Considerou, ainda, que os alunos foram devidamente informados sobre o tratamento de dados – que considerou lícito, nos termos da alínea *e)* do n.º 1 do art.º 6 do RGPD – e que a Universidade adotou as medidas de segurança técnicas e organizativas adequadas, no cumprimento do RGPD e da lei nacional de proteção de dados. Não se pronunciou, contudo, quanto ao facto de a Universidade alegadamente recolher alegadamente o consentimento dos alunos para aquele tratamento de dados, mas sem o qual não poderiam realizar o exame ou, ainda, sobre as transferências internacionais de dados efetuadas efetuadas no âmbito da utilização daquela solução comercial.

Atendendo à retrospetiva traçada, o presente estudo propõe-se a seguir um modelo para a categorização das soluções de avaliação a distância, por forma a melhor enquadrar as respetivas características e funcionalidade de cada uma s. De seguida, irão analisar-se os fundamentos de licitude elegíveis em cada tratamento de dados, concluindo-se quanto à necessidade de realização da avaliação de impacto sobre a proteção dos dados.

---

[19] "Universitets brug af tilsynsprogram ved online eksamen", Datatilsynet, disponível em: <*https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen*>.

[20] *Algoritmos e Estruturas de Dados*, por se tratar de uma prova em que as respostas corretas seriam idênticas, sem necessidade de desenvolvimento ou demonstração de resultados, exigindo-se que os alunos não comunicassem entre si.

2. Considerações prévias

O regime jurídico dos graus e diplomas do ensino superior, aprovado pelo Decreto-Lei n.º 74/2006, de 24 de março[21], prevê na sua redação atual, através das alíneas *e)* dos art.ºs 14.º e 26.º, que os regimes de avaliação de conhecimentos, respetivamente para o ciclo de estudos conducente ao grau de licenciado e de mestre, são aprovados pelo órgão legal e estatutariamente competente de cada estabelecimento de ensino superior.

No que concerne à modalidade de ensino superior a distância, o Decreto-Lei n.º 133/2019, de 3 de setembro, estabelece um quadro de princípios e regras de acreditação, organização e funcionamento das instituições de ensino superior que atuam sob esse modelo de ensino, delegando nas mesmas a definição das metodologias do processo de avaliação, que pode ser presencial, ou através de plataformas tecnológicas que assegurem a sua fiabilidade (cf. n.º 1 do art.º 14.º).

As instituições de ensino superior encontram-se, portanto, legitimadas para que possam optar, se assim o entenderem, por um regime de avaliação de conhecimentos a distância, desde que observem o cumprimento das respetivas normas e regulamentos de avaliação, sem prejuízo dos atos de supervisão e de (re)acreditação dos seus ciclos de estudos, designadamente pela Agência de Avaliação e Acreditação do Ensino Superior (A3ES)[22].

3. Soluções de monitorização: categorias e funcionalidades

As ferramentas que se propõem à monitorização da avaliação a distância fazem uso dos recursos do dispositivo do avaliado, entre os quais

[21] Alterado pelos Decretos-Leis n.ºs 107/2008, de 25 de junho, 230/2009, de 14 de setembro, 115/2013, de 7 de agosto, 63/2016, de 13 de setembro, 65/2018, de 16 de agosto e 27/2021, de 16 de abril.

[22] Criada pelo Decreto-Lei n.º 369/2007, de 5 de novembro.

se incluem a *webcam*, o microfone e a ligação à internet, podendo ser essencialmente enquadradas nas seguintes categorias[23], sem prejuízo da possibilidade da sua combinação entre si:

I. Monitorização em tempo real, com recurso a um ou mais avaliadores remotamente ligados, nos quais são delegadas as tarefas de verificação da identidade dos alunos e sua monitorização durante o período de realização da prova;

II. Monitorização com recurso à gravação de vídeo e, opcionalmente, também de áudio, através da qual se gravam os alunos durante o período de realização da prova. As gravações são posteriormente analisadas, geralmente por docentes, ou por terceiros contratados para o efeito;

III. Monitorização automática, na qual se procede à gravação dos avaliados durante a prova de avaliação. As gravações são automaticamente processadas por um sistema de análise de áudio e vídeo, para deteção e classificação de comportamentos suscetíveis de constituírem fraude académica.

As principais funcionalidades[24] disponibilizadas pelas soluções comerciais de monitorização são:

• Integração com sistemas de apoio ao ensino LMS (*learning management systems*), de onde se destacam as plataformas *Moodle*, *Blackboard* e *Canvas*. As provas de avaliação são criadas diretamente na plataforma de ensino, bem como a configuração da monitorização pretendida (*e.g.* gravar apenas vídeo, gravar áudio e vídeo, definir avisos prévios ao início da gravação, solicitar um documento de identificação);

---

[23] O'REILLY, Gordon e CREAGH, John, "A categorization of Online Proctoring", *Proceedings of Global Learn-Global Conference on Learning and Technology*, 2016, pp. 542-552.

[24] ARNÒ, Simone, GALASSI, Alessandra, TOMMASI, Marco e SAGGINO Aristide, "State--of-the-Art of Commercial Proctoring Systems and Their Use in Academic Online Exams", *International Journal of Distance Education Technologies*, Volume 19, Issue 2, April-June 2021, doi: 10.4018/IJDET.20210401.oa3.

• Autenticação/validação automática da identidade do aluno. Apesar do termo se encontrar cunhado em várias soluções, em muitas delas corresponde a um mero automatismo para solicitar e armazenar automaticamente o resultado da captura fotográfica de um documento de identificação exibido pelo aluno*(1). Como alternativa, ou complemento, poderá ser solicitada a validação de um código remetido para o endereço de correio eletrónico (institucional) do aluno, ou através da validação de uma conta de utilizador (nome e respetiva palavra-passe). Algumas soluções permitem, no entanto, uma verificação fiel do conceito de autenticação/verificação (biométrica), comparando, através do reconhecimento facial, um modelo (*template)* biométrico do aluno (previamente armazenado), com um outro que seja construído a partir de uma fotografia captada naquele momento. De igual modo, embora sem casos conhecidos, seria possível usar o mesmo princípio para o reconhecimento da voz do aluno, da sua impressão digital, íris, ou outros dados biométricos;

• Compatibilidade com dispositivos móveis iOS e/ou Android[25], enquanto meios complementares à monitorização do aluno e do espaço físico em que o mesmo se encontra;

• Restrição ao navegador *web* (*browser lockdown*)*(2), geralmente colocando-o em modo de 'ecrã-inteiro', e de específicas funcionalidades*(3) como a abertura de novos separadores, acesso a outras páginas *web* ou impressão de conteúdos;

• Restrição à execução de aplicações que não se revelem necessárias para realização da prova*(4), bem como de funcionalidades do sistema operativo (SO) e respetivos atalhos (*e.g.* copiar/colar, opções do botão direito do rato, fotografia de ecrã/*screenshot*)*(5);

• Deteção e restrição da tecnologia de virtualização*(6), evitando que o aluno execute outros sistemas operativos sobre aquele que proporciona a camada de virtualização (cf. Figura 1);

[25] Sistemas operativos para dispositivos móveis, respetivamente da *Apple* e da *Open Handset Alliance*.

• Gravação e/ou transmissão em tempo real de áudio e de vídeo do examinando. Possibilidade, consoante as aplicações, de sinalização de comportamentos suspeitos e dos respetivos instantes temporais, baseada na análise de movimentos com recurso à tecnologia de Inteligência Artificial;

• Procedimento automático, antes de se iniciar a prova de avaliação, para solicitar ao aluno que efetue uma rotação de 360.º com sua *webcam,* gravando um vídeo do local e das condições em que o exame será iniciado*(7);

• Gravação e/ou transmissão em tempo real, do conteúdo do monitor do examinando*(8);

• Captura e armazenamento do tráfego *web* gerado pelas aplicações, em ambos os sentidos (cliente/servidor e vice-versa)*(9);

• Restrição geográfica dos locais admissíveis para a realização do exame (*e.g.* via GPS);

• Transcrição de eventuais discursos captados pelo microfone;

• Término automático do exame, caso a solução considere (com certo grau de probabilidade) que o aluno adotou um comportamento classificado fraudulento;

• Comunicação em tempo real (*live chat*), entre vigilante e examinando.

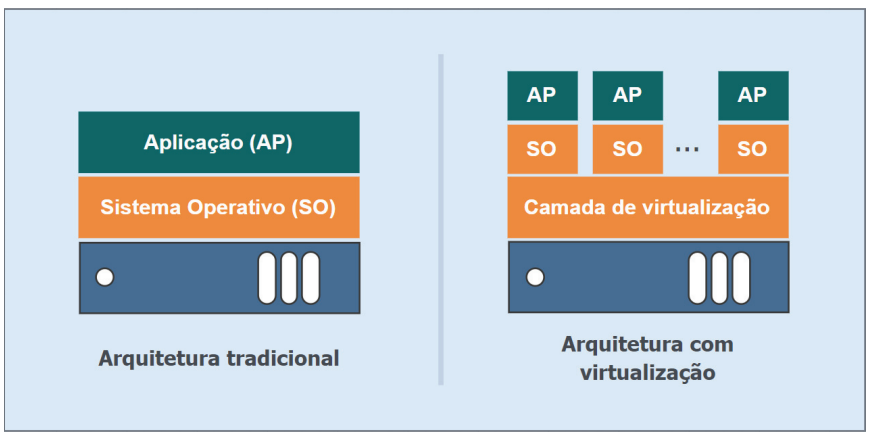

Figura 1 – Arquitetura tradicional e com virtualização.

É possível combinar a monitorização em tempo real com a monitorização automática, verificando-se, numa base contínua, a identidade do examinando e os seus comportamentos. Determinadas soluções, ao detetarem um comportamento suspeito (*e.g.* se o aluno tapar a boca com a mão) notificam de imediato o examinador que, através de um canal de comunicação (*live chat*), tem a possibilidade de alertar ou dar instruções ao aluno.

3.1. Exemplos de ferramentas e respetivas particularidades

Para observar as funcionalidades presentes em cada categoria de monitorização, analisaram-se sete ferramentas comerciais: *ExamNet, ProctorExam e Respondus,* – testadas no Piloto SAR[26] – *Jitsi, Colibri, Safe Exam Browser (SEB)* e *WISEflow* – pela sua ampla utilização e relevância para o estudo.

A informação relativa a cada uma das soluções foi verificada entre janeiro e fevereiro de 2023, através dos respetivos sítios *webe*, nos casos em que existiam, nos fóruns e *blogs* oficiais. Realça-se contudo, que à exceção das ferramentas de código aberto (*open source software*) *Jitsi* e SEB – cujo código não foi alvo de análise –, a informação disponibilizada sobre os específicos tratamentos de dados das várias funcionalidades das restantes soluções é praticamente inexistente ou fornecida de forma dispersa e, ainda assim, considerada pouco clara.

- *Jitsi*

Trata-se de uma plataforma *web* para realização de videoconferências. Pese embora exista uma aplicação para dispositivos móveis e que proporciona uma melhor experiência de utilização, é possível utilizar a solução em qualquer dispositivo sem necessidade da sua instalação, bastando para tanto aceder ao sítio[27] *web* do projeto, através de um navegador.

[26] Exclui-se da análise a solução francesa *TestWe*, por ser manifestamente insuficiente a informação publicamente disponível em: <*https://testwe.eu/pt*>.

[27] Disponível em: <*https://meet.jit.si*>.

A solução é disponibilizada pela empresa norte americana *8x8 Inc.*, de forma gratuita, porém, sem qualquer suporte ou garantia de serviço. O acesso ao código-fonte[28] é livre.

A solução trata os seguintes dados dos utilizadores: endereço IP, nome da sala virtual, conteúdos partilhados durante a sessão e número de contacto telefónico caso a ligação áudio seja estabelecida por via de chamada telefónica. De acordo com a informação disponibilizada, os conteúdos partilhados são apenas armazenados pelo tempo estritamente necessário (no caso das mensagens escritas até que a sessão de videoconferência termine; armazenamento da gravação da sessão, quando a mesma é ativada e até que esta seja totalmente transferida pelo utilizador)[29].

A plataforma permite efetuar uma videoconferência entre múltiplos participantes, que podem partilhar simultaneamente o conteúdo do seu monitor e o vídeo captado pela sua *webcam*. Paralelamente, pode ser efetuada a ligação através de outro dispositivo, o que permite obter imagens do aluno de outra perspetiva.

De acordo com a 'Política de Privacidade'[30], os dados tratados podem ser partilhados com entidades terceiras: "*We may disclose your personal information to the following categories of recipients: to any competent law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary (i) as a matter of applicable law or regulation, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person*".

- Colibri

É uma solução da FCT/FCCN[31] baseada na aplicação de videoconferência – norte americana – Zoom[32], permitindo a sua integração com

[28] Código aplicacional que, após compilado, dá origem à aplicação tal como a conhecemos.

[29] Informação disponível em: <*https://jitsi.org/meet-jit-si-privacy*>, [15 jan. 2023].

[30] "*Who does 8x8 share my personal information with?*", disponível em: <*https://www.8x8.com/terms-and-conditions/privacy-policy*>, [15 jan. 2023].

[31] Informação disponível em: <*https://ajuda.colibri.fccn.pt/sobre*>.

[32] Disponível em: <*https://zoom.us*>.

a plataforma de ensino *Moodle*. Foi inicialmente disponibilizado para permitir a realização de aulas e reuniões a distância. Após a conclusão do Piloto SAR foi também adotada, por diversas universidades, para monitorizar em tempo real[33] a avaliação dos alunos e, ainda, para a realização de provas públicas por videoconferência[34].

Por ser uma solução essencialmente pensada para a transmissão de conhecimento, a sua aplicação na monitorização da avaliação a distância apresenta certas limitações, mas também algumas vantagens face às demais. Enquanto que através do *Jitsi* é possível efetuar, na mesma sala virtual, a partilha simultânea da câmara e do conteúdo do monitor de todos os intervenientes, permitindo que a mesma pessoa possa vigiar vários alunos, no Colibri a partilha do monitor apenas pode ser efetuada por uma pessoa, em cada momento. No entanto, esta solução oferece a possibilidade de integração com o serviço de autenticação federada RCTSaai[35].

Embora o aluno necessite de instalar a aplicação *Zoom*, esta é atualmente disponibilizada para os sistemas operativos mais comuns, incluindo para dispositivos móveis, que podem ser utilizados de forma complementar. De acordo com a informação disponibilizada através do sítio *web*[36] e no Manual do Utilizador[37], o Colibri permite a gravação das sessões em *cloud,* sem especificar qual, aparentando essa escolha

[33] Utilizado pela Universidade de Coimbra (cf. informação disponível em: <*https://www.uc.pt/aerop/avaliacao_remota*>) e pela Universidade de Évora, que aconselhou os docentes a realizar as avaliações *online,* em tempo real, através do módulo do *Moodle* '*Safe Exam Browser*', com vigilância *Zoom/Colibri* por telemóvel, sem gravação (cf. Despacho reitoral n.º 8/2021, disponível em: <*https://gdoc.uevora.pt/695399*>).

[34] Cf. informação relativa à Universidade do Minho, disponível em: <*https://www.uminho.pt/PT/Teletrabalho/Paginas/ColibriProvasPublicas.aspx*>.

[35] A Rede Ciência Tecnologia e Sociedade (RCTSaai) é uma infraestrutura global de autenticação e autorização, através de uma conta institucional, destinando-se a alunos, docentes e funcionários das instituições aderentes (cf. informação disponível em: <*https://confluence.fccn.pt/display/RCTSAAI/RCTSaai*>).

[36] Disponível em: <*https://ajuda.colibri.fccn.pt/objetivo*>*,* [15 jan. 2023].

[37] 'Gravação das reuniões' (p.12), disponível em: <*https://videoconf-colibri.fccn.pt/assets/tutorial_colibri.pdf*>.

ser delegada na *Zoom Video Communications, Inc.*[38]. Os vídeos ficam disponíveis em *cloud* pelo período de 10 dias, durante o qual podem ser transferidas para o Portal Educast[39].

Ao utilizar a aplicação, sempre que os utilizadores se encontrem autenticados, são tratados os seguintes dados[40]: endereço IP, endereço de acesso à sala virtual[41], nome do utilizador, endereço de *e-mail*, relação entre o utilizador e a instituição de ensino (opcional), perfil do utilizador e conteúdos que o mesmo possa adicionar, modificar ou remover.

- *Safe Exam Browser (SEB)*

É um navegador *web* de características particulares, que permite definir e aplicar restrições à sua utilização, nomeadamente para realização de provas de avaliação (*e.g.* confinamento ao navegador/*browser lockdown,* inibição de certas funcionalidades do sistema operativo como a abertura de determinadas aplicações). A definição das restrições é geralmente comunicada por via da integração com um sistema LMS, de apoio ao ensino. É necessário que o navegador seja instalado no dispositivo do aluno, sendo este compatível com sistemas operativos Windows, macOS e iOS.

---

[38] De acordo com os termos de utilização do Colibri, disponíveis em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*> [4 fev. 2023], que mais não são do que a transposição dos termos de utilização da ferramenta *Zoom,* à data de 20 de agosto de 2020 (quando a versão atual, no sítio *web* da *Zoom,* é de 30 de dezembro de 2022), refere o ponto 3, relativo ao 'Uso dos serviços e suas responsabilidades', o seguinte: "O anfitrião pode escolher gravar reuniões e *webinars* da *Zoom*. Ao usar os Serviços, você dá consentimento à *Zoom* para armazenar gravações de toda e qualquer reunião ou *webinar* da *Zoom* em que você ingressar, caso sejam armazenadas em nossos sistemas.". Relembrando que a *Zoom Video Communications, Inc.*, enquanto detentora do produto *Zoom,* é uma empresa norte-americana, parece insuficiente a informação prestada pela FCT aos utilizadores da ferramenta, nomeadamente quanto ao local e às condições de armazenamento dos vídeos gravados, não só na *cloud* mas também no Portal Educast.

[39] Repositório de vídeos educativos nacionais e sua disponibilização aos alunos através da internet (disponível em: <*https://help.educast.fccn.pt/?page_id=372*>, [15 jan. 2023]).

[40] De acordo com a informação disponível em: <*https://ajuda.colibri.fccn.pt/termos-e-condicoes*>, [15 jan. 2023].

[41] Pode ser um dado pessoal se, para acesso à mesma sala virtual, forem enviados diferentes endereços consoante o utilizador final, permitindo relacionar um utilizador com o endereço que lhe foi disponibilizado.

O SEB permite também a integração (opcional) com as aplicações *Jitsi* e *Zoom*, conferindo assim uma componente de monitorização visual do aluno.

Segundo a informação publicada no sítio *web*[42], não existe recolha de dados pessoais pela aplicação: "*SafeExamBrowser (SEB) doesn't send any personal information to any centralized server and is not connected to any web analytics, user tracking or clickstream analytics service.*".

- *WISEflow*

Permite que os utilizadores se autentiquem na aplicação através da criação de uma conta, que pode ser criada por via da integração com vários serviços de autenticação federada, entre os quais o eduGAIN[43].

Requer que o utilizador instale um *plugin* no navegador *web Google Chrome,* permitindo a restrição de funcionalidades do navegador e do sistema operativo.

No início de cada prova de avaliação é tirada uma fotografia ao aluno, que vai sendo comparada com outras fotografias, posteriormente capturadas durante a realização da prova, em momentos aleatórios. Nas provas seguintes, não só são comparadas as novas fotografias que aí sejam capturadas, como também se as compara com aquelas que tenham sido captadas em provas anteriores, e que estão disponíveis pelo período de tempo definido pelo responsável pelo tratamento.

- *Exam.net*

É uma solução através da qual se podem criar as provas de avaliação, permitindo a correção de certo tipo de questões de forma automatizada. Possui, aquilo a que designa de três modos de segurança: no primeiro o aluno só pode realizar o teste através do *Safe Exam Browser,* com as

[42] Disponível em: <*https://safeexambrowser.org/about_overview_en.html#details*>.

[43] Serviço de autenticação disponibilizado a estudantes, investigadores e docentes das instituições de ensino aderentes. Disponível em: <*https://www.fccn.pt/noticias/edugain-conectar-o-mundo*>.

restrições que tenham sido definidas pela instituição de ensino; no segundo, o aluno pode recorrer a um qualquer navegador *web* para realização da prova; e no terceiro, apesar de se permitir a utilização de outros navegadores, é dada preferência, de forma automática, ao SEB.

Para aceder ao exame os alunos não necessitam de criar uma conta *ExamNet*, bastando a introdução de um código que lhes é previamente remetido.

São referidas outras funcionalidades da solução, sem especificar que informação é recolhida acerca do aluno, ou do seu dispositivo: "Também temos deteção de fraude em *background*, que ocorre a um nível mais profundo nos nossos servidores. Isso permite-nos detetar discretamente e informar docentes de suspeita de fraude tal como o uso de *software* especial, ecrãs divididos, *hacking* à integridade do nosso código (ou do ambiente) e procuramos a utilização de máquinas virtuais e soluções de ambiente de trabalho remotas. A nossa equipa monitoriza e afina frequentemente os módulos de deteção de fraude, acompanhando o que acontece no mundo real."[44].

- *Respondus (Monitor* e *LockDown Browser)*

É uma solução composta pelas vertentes de análise (*Monitor)* e de restrição de funcionalidades (*LockDown Browser*). Permite ativar funcionalidades de monitorização em função do tipo de prova[45]:

a) Avaliação na sala de aula, em modo *online,* sem necessidade de recorrer à utilização de *webcams*. O docente fica incumbido de vigiar os alunos presencialmente, enquanto a componente *LockDown Browser* restringe o ambiente da prova àquele navegador, validando o acesso à prova por via de palavra-passe.

b) Avaliação a distância com monitorização automática, através das componentes *LockDown Browser* e *Monitor.* A primeira confere as capacidades anteriormente descritas, enquanto que a segunda guia o

[44] Disponível em: <*https://exam.net/pt/cheat*>, [15 jan. 2023].

[45] Disponível em: <*https://web.respondus.com/wp-content/uploads/2021/03/RespondusMonitor_Scenarios.pdf*>.

aluno na verificação das condições de ligação à *internet* e de funcionamento da *webcam*, bem como na verificação da sua identidade[*(1)]. Após a prova, o docente verifica os resultados fornecidos pela ferramenta, que assinala os instantes temporais das práticas suscetíveis de constituírem fraude, disponibilizando o vídeo respetivo[46].

c) Avaliação em tempo real, sem gravação ou deteção automática de comportamentos suspeitos, na qual o aluno realiza a prova a distância, com recurso à componente *LockDown Browser*. É monitorizado pelo docente, através de uma sessão de videoconferência com recurso às ferramentas *Zoom*, *Teams ou Meet*.

d) Avaliação que combina, simultaneamente, alunos em regime presencial e a distância. Os métodos de monitorização aplicados são, respetivamente, os descritos nas alíneas *a)* e *c)*.

Existe uma funcionalidade designada *Photo on File*, que permite às instituições de ensino carregar fotografias dos alunos, ou dos respetivos documentos de identificação[47]. O propósito é o de permitir identificar quem realiza o exame. No entanto, não é referido se a comparação pode ser automatizada, envolvendo o tratamento de dados biométricos.[*(10)]

De acordo com a política de tratamento de dados[48], a *Respondus, Inc.* tem como subcontratantes a *Amazon Web Services, Inc.*, para prestação do serviço de armazenamento de dados, e a *PayPal* para o processamento de pagamentos, reservando-se o direito de alterar a lista de subcontratantes, em qualquer momento, bastando que reflita as alterações no sítio *web* por si indicado[49]. No ponto 2.3, relativo às transferências internacionais de dados, é dado a conhecer que os dados são tratados fora do Espaço Económico Europeu (incluindo o seu

[46] Motivo, pelo qual, se considera suportar a monitorização com recurso à gravação de vídeo.

[47] Disponível em: <*https://support.respondus.com/hc/en-us/articles/4409607197211-What-is-the-Photo-on-File-feature-that-appears-in-the-instructor-s-video-review-section-*>.

[48] Disponível em: <*https://web.respondus.com/data-processing*>.

[49] Disponível em: <*https://web.respondus.com/privacy/subprocessors*>.

armazenamento), cabendo ao responsável pelo tratamento a tarefa de recolher, junto dos titulares, o respetivo consentimento. O ponto 2.4, relativo às medidas de segurança, menciona a utilização de técnicas de pseudonimização e de cifra, mas não de anonimização dos dados, e sem que referira a que dados ou em que medida são aplicadas as técnicas mencionadas.

Os vídeos gravados pela solução são geralmente armazenados por um período de cinco anos, a partir da data da sua gravação, a menos que o responsável pelo tratamento solicite um prazo de conservação diferente[50].

- *ProctorExam*

Entre o período de realização do Piloto SAR e a atualidade, a solução passou de uma infraestrutura no centro de dados do responsável pelo tratamento (*on-premises*) para um modelo de computação na nuvem (*cloud computing*), socorrendo-se dos serviços prestados pelos subcontratantes *Amazon Web Services* e *Google Cloud.*

Para utilizar a solução é necessário que o aluno instale um *plugin*[51] específico para o navegador *Google Chrome.*

Segundo o sítio *web* da solução[52], são geralmente tratados os seguintes dados do examinando: nome; endereço de *e-mail;* número de estudante ou outro número de identificação pseudonimizado; vídeos e outros dados relativos à gravação do conteúdo do monitor e por via da *webcam* (incluindo da câmara do telemóvel quando utilizado como dispositivo secundário); rosto do estudante e ambiente envolvente; e identificação da instituição de ensino. Na secção '*Data we collect automatically when you use ProctorExam'*, é referida a 'possibilidade' de tratamento de informação relativa ao navegador *web*, sistema operativo

[50] Disponível em: <*https://support.respondus.com/hc/en-us/articles/4409595425307-How-long-is-video-kept-What-if-we-need-a-longer-period-*>.

[51] Disponível em: <*https://chrome.google.com/webstore/detail/proctorexam-screen-sharin/digojkgonhgmnohbapdfjllpnmjmdhpg*>.

[52] Informação disponível em: <*https://proctorexam.com/privacy-and-data-security*>, [12 jan. 2023].

e do endereço IP[53] do examinando, como que não constituindo, também ela, dados pessoais.

A tabela seguinte relaciona as características e funcionalidades das soluções descritas, em função da(s) sua(s) categoria(s) de monitorização.

Características e Funcionalidades			Jitsi	Colibri	SEB	WISEflow	ExamNet	Respondus	ProctorExam
Gerais	Infraestrutura		local/*cloud*	*cloud*	*local*	*cloud*	*cloud*	*cloud*	*cloud*
	Subcontratantes		✓	✓		✓	✓	✓	✓
	Integração LMS		✓	✓	✓	✓	✓	✓	✓
	Conversação *(live chat)*		✓	✓			✓		
	Instalação p*lugin web*					✓			✓
	Instalação aplicação			✓	✓		✓	✓	
	Open Source		✓		✓				
	Sede da empresa		EUA	PT/EUA	Suíça	Dinamarca	Suécia	EUA	Países Baixos
Autenticação	Documento de identificação	*(1)						✓	✓
	Reconhecimento facial					✓		✓	
	Padrão de escrita							✓	
	Por videoconferência		✓	✓	✓		✓	✓	
	Foto em ficheiro	*(10)						✓	
Restrição	Ao navegador *web*	*(2)			✓	✓	✓	✓	
	Opções do navegador *web*	*(3)			✓	✓	✓	✓	✓
	Execução de aplicações	*(4)			✓	✓	✓	✓	
	Funcionalidades do SO	*(5)			✓	✓	✓	✓	
	Virtualização	*(6)			✓	✓	✓	✓	
Monitorização	**Monitorização em tempo real**		✓	✓	✓		✓	✓	✓
	Gravação áudio/vídeo		✓	✓				✓	✓
	Monitorização automática					✓		✓	
	Meio envolvente	*(7)						✓	✓
	Monitor do aluno	(8)	✓	✓					
	Captura do tráfego *web*	*(9)							
	Suporta *webcam* secundária		✓	✓					✓
Compatível	MS Windows	Desktop	✓	✓	✓	✓	✓	✓	✓
	Linux	Desktop	✓	✓					✓
	macOS	Desktop	✓	✓	✓	✓	✓	✓	✓
	Android	Móvel	✓	✓					✓
	iOS	Móvel	✓	✓	✓	✓	✓		✓

Tabela 1 – Características e funcionalidades das soluções de monitorização descritas, em função da sua categoria.

[53] No Acórdão do TJEU, relativo ao processo C-582/14 (*Patrick Breyer v Bundesrepublik Deutschland*), o Tribunal reconheceu que sob certas circunstâncias, um endereço de IP dinâmico é um dado pessoal, mesmo quando a informação adicional, que permite a identificação do titular, se encontra na posse do provedor de serviços/*internet service provider* (ISP). As circunstâncias a que se refere o Tribunal correspondem à possibilidade de se combinar informação adicional que permita identificar o titular dos dados, o que se verifica neste caso.

A necessidade de instalação de uma aplicação no dispositivo do aluno e/ou de um *plugin* para o navegador *web* é, geralmente, um requisito transversal às soluções dos três modelos de monitorização. Pela sua capacidade de funcionamento através das funcionalidades dos navegadores *web*, o projeto *Jitsi* é uma exceção à regra, permitindo a monitorização em tempo real e/ou com recurso à gravação, sem necessidade de qualquer instalação[54] pelo aluno.

As soluções que requerem a instalação de uma aplicação, visam sobretudo a compatibilidade com sistemas operativos *Microsoft Windows* e *Apple macOS.* Por esse motivo, haverá que salvaguardar que da sua utilização não resultam ónus para os alunos, nomeadamente relativos aos custos de licenciamento e de instalação de um sistema compatível, quando estes possuam um outro[55].

De um modo geral, com especial predominância nas soluções que conferem monitorização automática, observa-se uma elevada adesão a serviços prestados por terceiros. Este facto, tem essencialmente que ver com duas ordens de razão:

- Por um lado, a tendência natural de migração para um modelo de computação na nuvem[56], por aí se encontrar resposta ao elevado consumo – mas também variável – de recursos computacionais, que a tecnologia de Inteligência Artificial tanto exige. A adesão à computação em nuvem permitiu, ainda, centralizar a infraestrutura de suporte à respetiva solução, contribuindo para a abstração de um conjunto de tarefas complexas de gestão e manutenção, não só da infraestrutura de suporte como da própria solução. A disponibilidade das soluções e sua resiliência a falhas passou a ser praticamente inabalável, enquanto que o responsável pelo tratamento passou (apenas) a configurar os mecanismos de segurança que pretende conferir a cada prova de avaliação.

[54] Tipicamente os sistemas operativos incluem já um navegador *web*.

[55] Pelo menos nos casos em que a opção pela avaliação a distância não tenha partido do próprio aluno. Mas, ainda que fosse essa a sua vontade, seria expectável que o aluno fosse informado, *a priori,* dos exatos termos de funcionamento da solução, de onde se incluem os requisitos da sua instalação.

[56] Que pode ser total, ou híbrido (migração de apenas parte dos serviços).

• Por outro lado, a disponibilização no mercado de funcionalidades de eficácia comprovada e de grande utilidade na automatização da monitorização, permitindo reduzir drasticamente o esforço de desenvolvimento e manutenção das soluções. São disso exemplo as funcionalidades de reconhecimento facial e de voz, ou a transcrição de discursos, disponibilizadas pela *Amazon Web Services* (AWS)[57].

As soluções de monitorização automática implicam o tratamento de dados biométricos por recorrerem, entre outras, a técnicas de reconhecimento facial, as quais implicam riscos acrescidos para os direitos dos titulares dos dados[58].

A informação disponibilizada pela generalidade das soluções nos respetivos sítios *web* é, geralmente, insuficiente para que responsável pelo tratamento (*a priori*) ou titulares dos dados (*a posteriori*), conheçam com rigor as técnicas e os dados tratados por determinada solução, no seu modelo base de funcionamento (*i.e.* sem a implementação de requisitos impostos).

A decisão de subcontratação impõe que se estabeleça uma negociação entre as partes que, no entanto, pelo facto de algumas soluções serem altamente dependentes de determinadas tecnologias, ou de serviços de terceiros, dificultam em muito certas intenções de alteração ao funcionamento da solução.

A ausência de medidas de proteção de dados desde a conceção poderá igualmente ter consequências diretas nas medidas de proteção de dados por defeito, que o responsável pretenda conferir[59].

---

[57] "How the cloud can help educational institutions with grading, assessments, and admissions", *AWS Public Sector Blog,* (em linha), disponível em: <*https://aws.amazon.com/blogs/publicsector/how-cloud-can-help-educational-institutions-grading-assessments-admissions*>.

[58] Cf. ponto 73 das Diretrizes 3/2019 do CEPD, sobre tratamento de dados pessoais através de dispositivos de vídeo (em linha), disponível em: <*https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf*>.

[59] Naquela que foi a intenção de adotar a solução *Respondus,* por parte de uma instituição de ensino superior portuguesa que, contudo, não pretendia a captação de som, viu-se a mesma obrigada a criar manuais para instruir os alunos a desativar o microfone, através do respetivo sistema operativo. Esta medida resultou de uma manifesta ausência de medidas de proteção dos dados desde a conceção e, por consequência, por defeito. É, ainda, um exemplo daquilo que não foi possível ultrapassar por via de um suposto processo de negociação de subcontratação.

Parte desses dados não são sequer percecionados, pelos subcontratantes, enquanto dados pessoais, apesar da sua combinação permitir a identificação de uma pessoa[60]. Não obstante, importará referir que é ao responsável pelo tratamento que cabe assegurar-se de que o tratamento é realizado em conformidade com o RGPD (cf. art.º 24.º do mesmo diploma), a quem compete, também, despojar-se de quaisquer dúvidas ou incertezas antes de adotar uma determinada solução de monitorização.

4. Fundamentos de licitude para o tratamento de dados pessoais

As soluções de monitorização são tão atraentes quanto melhor se revele a sua eficácia na prevenção e deteção de fraude académica. A opção por soluções de monitorização automática, por implicar o tratamento de dados biométricos, carece de especial atenção no momento da sua fundamentação.

No que respeita aos fundamentos jurídicos para o tratamento de dados pelos diferentes modelos de monitorização, analisaremos conjuntamente a monitorização em tempo real e com recurso à gravação de vídeo, e em secção própria a monitorização automática.

4.1. Tratamento de dados nos processos de monitorização não automáticos

Para o tratamento de dados associado aos modelos de monitorização em tempo real e com recurso à gravação de vídeo perfilam-se, à partida, as alíneas *a)*, *e)* ou *f)* do n.º 1 do art.º 6.º do RGPD[61].

[60] Vide considerações, anteriormente tecidas, acerca da solução *ProctorExam.*

[61] Respetivamente: se o titular dos dados tiver dado consentimento para o tratamento dos seus dados pessoais, para a(s) finalidade(s) em causa; 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; ou se o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, a menos que prevaleçam os interesses ou direitos e liberdades fundamentais do titular dos dados.

Em qualquer das hipóteses, teria o responsável pelo tratamento de adotar as medidas técnicas e organizativas necessárias para mitigar os riscos associados à gravação não autorizada e ao acesso indevido às gravações autorizadas, que necessitariam de ter associado um prazo de conservação previamente estabelecido[62] A par da obrigatoriedade do cumprimento dos restantes princípios relativos ao tratamento de dados, entende-se que seria útil a aprovação de um código de conduta e de um manual de procedimentos destinados aos vigilantes, contribuindo assim para uma atividade idónea e limitada às finalidades do tratamento dos dados[63].

4.1.1. Consentimento do titular dos dados

Remetendo-nos ao fundamento jurídico previsto na alínea *a)* do n.º 1 do art.º 6.º do RGPD, entende-se que o consentimento do aluno (que se supõe maior de idade) afigura-se condição suficiente para o tratamento dos dados desde que prestado nas condições do disposto no ponto 11 do art.º 4.º do RGPD, na sua redação atual[64], bem como cumpridos os princípios relativos ao tratamento de dados pessoais (art.º 5.º, *ibid*.).

Note-se, no entanto, que o Considerando n.º 43, do RGPD, classifica de improvável a livre vontade do titular, sempre que se verifique um manifesto desequilíbrio entre o titular dos dados e o responsável pelo seu tratamento, designadamente quando este se trate de uma autoridade pública. Um consentimento efetivamente livre implicaria sempre que fosse dada ao aluno a possibilidade de realizar a mesma prova em regime presencial, o que poderia não ser imediatamente praticável, num contexto em que vigorassem restrições aos direitos dos cidadãos (*e.g.* durante a pandemia por COVID-19).

---

[62] Cf. n.º 1 do art.º 24.º do RGPD, relativo à responsabilidade do responsável pelo tratamento. Alíneas *e)* e *f)*, n.º 1 do art.º 5.º do RGPD, relativas ao princípio da limitação da conservação e ao princípio da integridade e confidencialidade dos dados, respetivamente.

[63] Respetivamente, art.º 5.º e n.º 2 do art.º 24.º, ambos do RGPD.

[64] A segunda retificação ao Regulamento Geral sobre a Proteção de Dados, publicada no jornal oficial da União a 4 de março de 2021, substitui a expressão «explícita» por «inequívoca».

Por esse motivo, de acordo com as Diretrizes n.º 5/2020 do CEPD (pontos 16 e 17)[65], relativas ao consentimento na aceção do Regulamento 2016/679, o tratamento de dados baseado na alínea *e)* do n.º 1 do art.º 6 do RGPD parece ser, neste tipo de casos, o mais apropriado. É o que se analisa em seguida.

4.1.2. Tratamento por motivos de interesse público

Os interesses prosseguidos pelas entidades públicas correspondem aos interesses públicos determinados por lei[66].

No caso das instituições públicas de ensino superior ministrado a distância, prevê o disposto no art.º 14.º do Decreto-Lei n.º 133/2019, de 3 de setembro, que cabe a estas "definir metodologias de avaliação formativa e sumativa que integrem avaliações presenciais ou através de plataformas tecnológicas, que assegurem a fiabilidade da avaliação desenvolvida".

No que concerne às restantes instituições públicas de ensino superior, prevê o Decreto-Lei n.º 74/2006, de 24 de março, na sua redação atual, que os regimes de avaliação de conhecimentos são aprovados pelo órgão legal e estatutariamente competente do respetivo estabelecimento de ensino. Desta forma, seria suficiente contemplar os modelos de avaliação em tempo real e/ou com recurso à gravação nas respetivas normas e regulamentos de avaliação, bem como a publicação do respetivo despacho reitoral de homologação[67].

---

[65] Disponível em: <*https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf*>.

[66] Regime jurídico das instituições de ensino superior, aprovado pela Lei n.º 62/2007, de 10 de setembro.

[67] Vide exemplos em nota de rodapé n.º 33 e 34.

4.1.3. Tratamento por motivo de interesses legítimos do responsável

O segundo parágrafo[68] do n.º 1 do art.º 6.º do RGPD veda às autoridades públicas, na prossecução das suas atribuições, a possibilidade de fundamentar o tratamento de dados com base na alínea *f)* do primeiro parágrafo, *ibidem*.

As instituições privadas de ensino superior regem-se pelo direito privado, em tudo o que não for legalmente contrariado[69]. A alínea *f)* do n.º 1 do art.º 6.º do RGPD é assim uma opção válida para este tipo de instituições que, contudo, sempre teriam que demonstrar a impossibilidade de realizar a avaliação por outra via, que não envolvesse o tratamento de dados pessoais em medida que ultrapassasse a da avaliação presencial. É, pois, o que se retira da conjunção dos três primeiros princípios do RGPD[70] relativos ao tratamento de dados pessoais, *i.e.,* revestir o tratamento de um caráter de necessidade, circunscrito ao mínimo indispensável para prossecução das finalidades (que devem ser lícitas) e limitado ao tratamento de dados adequados, pertinentes e necessários a essas mesmas finalidades.

Por outro lado, seria condição *sine qua non* a realização de um teste de adequação do qual não resultasse que os interesses, direitos e liberdades dos titulares dos dados não prevaleceriam sobre os interesses legítimos do responsável pelo tratamento.

Quanto às fundações públicas sujeitas a um regime de direito privado, fundamentou a CNPD o seu ponto de vista na Deliberação/2021/662 (pontos 46 a 50). Daí se retira que, às fundações que tenham por

---

[68] Apesar de não ser relevante para este caso, note-se que a versão portuguesa do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho é a única que refere no segundo parágrafo do art.º 6.º (*in fine*), a expressão "por via eletrónica", presumindo-se tratar de uma gralha. *Nova Legislação de Proteção de Dados*, CNPD, dez. 2019, depósito legal n.º 466370/20.

[69] Cf. n.º 4 do art.º 9.º da Lei n.º 62/2007 (Regime jurídico das instituições de ensino superior).

[70] Alíneas *a)*, *b)* e *c)* do n.º 1 do art.º 5.º do RGPD, respetivamente: licitude, lealdade e transparência; limitação das finalidades e; minimização dos dados.

missão a manifesta prossecução do interesse público, estará, em princípio, vedada a invocação de interesses legítimos.

4.2. Monitorização automática e o tratamento de dados biométricos

A monitorização automática está geralmente associada à utilização de técnicas de reconhecimento facial para validação da identidade do aluno, implicando, por esse motivo, o tratamento de dados biométricos[71]. De uma análise ao Considerando n.º 51 do RGPD, *prima facie*, resultará o entendimento de que o tratamento de fotografias constitui um tratamento de categorias especiais[72] de dados pessoais, sempre que "processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular", sendo abrangidas pela definição de dados biométricos.

Segundo o entendimento de A. Barreto Menezes Cordeiro, os Considerandos não podem ser utilizados para diminuir ou aumentar o alcance da lei, sendo o seu único propósito o de explicar os preceitos legais e os motivos que os sustentam. Nesse sentido, sendo perentório o n.º 1 do art.º 9 do RGPD na proibição de tratamento dados biométricos "para identificar uma pessoa de forma inequívoca", o Considerando n.º 51 mais não vem do que esclarecer que essa proibição abrange tanto as técnicas de identificação como de autenticação/verificação biométricas.

[71] Dados biométricos, segundo a alínea *14)* do art.º 4.º do RGPD, "são dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos."

[72] Que, de acordo com n.º 1 do art.º 9.º do RGPD, inclui os "dados biométricos para identificar uma pessoa de forma inequívoca".

Para clarificar a diferença entre os conceitos, atente-se no Parecer n.º 3/2012 do WP29[73] (p.6)[74] sobre a evolução das tecnologias biométricas, de onde se extrai, sobre a identificação biométrica:

"[a] identificação de uma pessoa por um sistema biométrico consiste, em regra, no processo de comparação de dados biométricos dessa pessoa (obtidos no momento da identificação) com um determinado número de modelos biométricos armazenados numa base de dados (ou seja, um processo de correspondência «um para muitos»)".

A definição anterior encontra-se em linha com a posição da Comissão Europeia patente no Livro Branco sobre a Inteligência Artificial (p.24)[75], no qual se expõe que a "identificação significa que o modelo da imagem facial de uma pessoa é comparado com muitos outros modelos armazenados numa base de dados para saber se a imagem dessa pessoa se encontra armazenada nessa base de dados".

O conceito parece, assim, estar associado ao processo de comparação de um determinado modelo (*template*) biométrico de uma pessoa desconhecida, ou para a qual não se sabe se estará registada na base de dados, daí resultando a necessidade de comparação com os vários modelos biométricos que constituem a base de dados (*e.g.* leitores biométricos para controlo de assiduidade ou de acesso a instalações).

Relativamente à verificação (ou autenticação) biométrica, refere o no Parecer n.º 3/2012 do WP29, o seguinte:

"[a] verificação de uma pessoa por parte de um sistema biométrico consiste, em regra, no processo de comparação de dados biométricos dessa pessoa (obtidos no momento da identificação) com um único

[73] Grupo de trabalho previsto pelo art.º 29.º da Diretiva 95/46/CE, para dar orientações gerais na clarificação da legislação em matéria de proteção de dados. Lidou com as questões relativas à proteção de dados pessoais e à privacidade até 25 de maio de 2018, data de em que a Diretiva 95/46/CE foi revogada pela execução do RGPD e o WP29 substituído pelo Comité Europeu para a Proteção de Dados (EDPB, na versão inglesa).

[74] Disponível em: <*https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf*>.

[75] Disponível em: <*https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1*>.

modelo biométrico armazenado num dispositivo (ou seja, um processo de correspondência «um para um»)".

O Livro Branco sobre a Inteligência Artificial descreve o mesmo conceito como a "comparação de dois modelos biométricos, que geralmente se pressupõe pertencerem à mesma pessoa (…) para determinar se a pessoa que aparece nas duas imagens é a mesma", dando como exemplo o controlo automatizado de fronteira nos aeroportos.

A título de exemplo, considere-se o processo de verificação existente nos *smartphones* e que permite criar um modelo biométrico com base em fotografias do seu proprietário. Posteriormente, é possível ao proprietário desbloquear o equipamento se, da verificação entre a fotografia tirada naquele momento e o modelo biométrico previamente criado, resultar uma relação de correspondência.

De referir, ainda, que diversas soluções de monitorização automática garantem a validação da identidade do aluno não só através de técnicas de reconhecimento facial, como também por via do tratamento de outros dados biométricos. Aí se enquadrará a análise do padrão de escrita do aluno, ou dos seus dados comportamentais, que contribuem igualmente para o grau de sucesso da sua identificação de forma inequívoca.

Relembrar, também, que essa identificação ocorre não só no momento que antecede a prova, mas também durante o período da sua realização, no qual são capturadas novas amostras, que por sua vez poderão ter a dupla finalidade de servir uma comparação imediata ou, a partir delas, se aperfeiçoar ou criar novos modelos biométricos para futuras comparações (cf. sucede com a solução *Wiseflow*).

Pelos motivos expostos, as soluções de monitorização automática terão de ser abordadas na perspetiva do tratamento de categorias especiais de dados pessoais, exigindo-se, nesse contexto, a verificação de uma das exceções previstas no n.º 2 do art.º 9.º do RGPD, que permita o levantamento da proibição prevista no n.º 1 do mesmo artigo e diploma.

4.2.1. Consentimento explícito do titular dos dados

O consentimento explícito do titular dos dados é a possibilidade prevista pela alínea *a)* do n.º 2 do art.º 9.º do RGPD, salvo se o direito da União ou do Estado-Membro previr que a proibição do tratamento dos dados não possa ser levantada. Não parece ser esse o caso, atenta a Lei n.º 58/2019, de 8 de agosto, e tendo em conta que o público alvo serão alunos do ensino superior, supondo-se maiores de idade.

O consentimento do aluno afigura-se condição suficiente para o tratamento dos seus dados biométricos, desde que seja livre, específico, informado e inequívoco, na aceção do disposto no ponto 11 do art.º 4.º do RGPD, mas também ele explícito, atendendo ao tratamento de categorias especiais de dados pessoais, e desde que cumpridos os princípios relativos ao tratamento de dados pessoais (art.º 5.º do mesmo diploma).

No entanto, para que o consentimento seja efetivamente livre, sendo essa uma condição essencial para que se considere válido, o ponto 3 das Diretrizes 05/2020 refere que "o consentimento só pode constituir fundamento jurídico adequado se, ao titular dos dados, for oferecido controlo e uma verdadeira opção de aceitar ou recusar os termos propostos ou recusá-los sem ser prejudicado".

Tendo em conta que o aluno não se encontra numa posição de paridade em relação ao estabelecimento de ensino que frequenta, o seu consentimento só será efetivamente livre[76] se, à luz dos Considerandos n.º 42 (*in fine*) e 43 do RGPD, lhe for concedida a possibilidade de realizar a mesma prova de avaliação sem se sujeitar a tais medidas de controlo. Assim, seria válida a alternativa de realização da atividade de avaliação em regime presencial, ou outra forma, desde que não implicasse o tratamento de dados biométricos, e praticada em iguais circunstâncias de dificuldade, sem que optando por uma dessas soluções resultassem consequência negativas para o aluno.

[76] De acordo com o ponto 13 das Diretrizes 05/2020 do CEPD, "[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".

4.2.2. Tratamento por motivos de interesse público

O levantamento da proibição do tratamento de dados biométricos poderá ainda acontecer nas condições a que se refere a alínea *g)* do n.º 2 do art.º 9.º do RGPD. No entanto, o fundamento referido não só requer a existência de interesse público, como o classifica de 'importante', característica que não lhe está associada em qualquer outra disposição do RGPD, vincando assim um atributo que alça uma especial necessidade de proteção dos dados tratados.

Atento o disposto no art.º 14.º do Decreto-Lei n.º 74/2006, de 24 de março, tal norma, que define a autonomia do respetivo órgão legal e estatutariamente competente para aprovar o regime de avaliação de conhecimentos não será condição suficiente para permitir a utilização de técnicas de reconhecimento facial nos processos de avaliação, não obstante a natureza do interesse prosseguido.

Pelo facto de o tratamento incidir sobre categorias especiais de dados pessoais, sendo suscetível de provocar maior risco de ingerência nos direitos fundamentais[77] dos alunos, será necessário que se encontre legalmente estatuído em que medida e circunstâncias, sem esquecer as salvaguardas adequadas, se poderá identificar os estudantes com recurso aos seus dados biométricos (Considerando n.º 52 do RGPD).

Ao verificar-se a situação anteriormente descrita, seria igualmente expectável a regulamentação (*e.g.* através da publicação de uma Portaria), das especificidades (da utilização) a que se referem as Orientações sobre Reconhecimento Facial[78] do Comité Consultivo[79] da

[77] Incluindo, mas não limitado ao respeito pela vida privada e familiar e ao direito à proteção de dados pessoais (respetivamente, art.º 7.º e 8.º da Carta dos Direitos Fundamentais da UE), de acordo com as considerações da Agência dos Direitos Fundamentais da União Europeia sobre a tecnologia de reconhecimento facial. Não se tratando de direitos absolutos, poderão os mesmos ser sujeitos a interferências devidamente justificadas, desde que não comprometam os valores fundamentais e inalienáveis desses direitos.

[78] "*Guidelines on facial recognition*", Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), 2021. Disponível em: <*https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html*>.

[79] Previsto no Capítulo V (parágrafos 85 a 87) da Convenção 108, de 1981.

Convenção 108[80], tendo em conta que o Estado Português aderiu à referida Convenção em 14 de maio de 1981, ratificando-a em 2 de setembro de 1993. A partir de 1 de janeiro de 1994 passou a mesma a ser executada na ordem jurídica nacional.

O tratamento dos dados por motivos de interesse público parece ser, aliás, o caminho adequado, quando em causa esteja a restrição de direitos fundamentais dos titulares, uma vez que o Considerando n.º 52 do RGPD prevê que a derrogação possa ser feita por motivos de ordem sanitária, incluindo de saúde pública – como se verificou em abril de 2020 e nos tempos que se seguiram. Ainda assim, haveria que criar o referido diploma em respeito pelos princípios da necessidade e proporcionalidade, sem esquecer as salvaguardas adequadas, submetendo-o ao parecer prévio da CNPD (embora não vinculativo), no âmbito das suas atribuições e competências.

5. Da necessidade de realizar uma AIPD

A realização de uma avaliação de impacto sobre a proteção de dados (AIPD)[81] permite ao responsável pelo tratamento – em princípio a instituição de ensino, a menos que essa responsabilidade seja (explicitamente) partilhada – não só avaliar os riscos que o tratamento é suscetível de gerar, como ainda, o auxilia na gestão desses riscos, permitindo avaliar e garantir a necessidade e a proporcionalidade do tratamento dos dados. Tem, portanto, uma dupla finalidade.

Exige-se a realização de uma AIPD sempre que um tratamento – em particular se utilizar novas tecnologias, e atendendo à sua natureza, âmbito, contexto e finalidade – seja suscetível de implicar um elevado

[80] Convenção para a Proteção de Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, *European Treaty Series* n.º 108, pp. 7-8, *in fine*. Disponível em: <*https://rm.coe.int/16800ca434*>.

[81] Cujo conteúdo mínimo se encontra descrito no n.º 7 do art.º 35.º do RGPD.

risco para os direitos e liberdades dos titulares[82]. A realização de AIPD é obrigatória, mas não limitada, aos casos em que se verifique o tratamento de categorias especiais de dados em grande escala[83].

5.1. Tratamento de dados nos processos de monitorização não automática

Ainda que possa não se entender obrigatória a realização de AIPD nos tratamentos de dados prosseguidos pelos métodos de monitorização em tempo real e com recurso à gravação, a opção pela sua efetiva realização irá favorecer, em primeiro lugar, o responsável pelo tratamento, ao muni-lo dos dados necessários a atestar a conformidade do tratamento e, por último, os titulares dos dados e a defesa dos seus direitos e liberdades.

Nessa análise devem versar as conclusões sobre os riscos associados à utilização de determinada solução comercial (ou desenvolvida pela própria instituição), e as medidas adotadas para mitigar esses mesmos riscos.

Note-se, porém, que se os tratamentos anteriores forem prosseguidos sob determinadas circunstâncias, poderão efetivamente requerer a realização de uma AIPD. É, pois, essa a responsabilidade do responsável pelo tratamento. A título de exemplo tome-se um caso de monitorização com recurso à gravação que envolva transferências internacionais de dados para o território de um país terceiro que não assegure um nível de proteção de dados adequado, nomeadamente para o armazenamento dos vídeos. Deverão ser adotadas salvaguardas adicionais (*e.g.* cifra das comunicações e dos dados armazenados) para garantir um nível de proteção dos dados essencialmente equivalente ao da União Europeia[84], sendo óbvia, nesse caso, a necessidade de realizar uma AIPD.

---

[82] Cf. n.º 1 do art.º 35.º do RGPD.

[83] Cf. alínea *b)* do n.º 3 do art.º 35.º do RGPD.

[84] Por referência ao Acórdão do TJUE, de 16 de julho de 2020, no processo C-311/18 (Acórdão *Schrems II*).

Nos casos em que a instituição de ensino determina aos alunos a instalação de específicas aplicações nos seus dispositivos, pois então esta terá necessariamente a responsabilidade de fazer o que estiver ao seu alcance para garantir que essas aplicações sejam seguras, não só naquele momento, como em utilizações futuras. Parece assim razoável, sem prejuízo de outras garantias ou intervenientes, a delegação de responsabilidade no subcontratante e contratualmente assumida, para que este realize os testes necessários à segurança da aplicação, numa base contínua, dando deles conhecimento ao responsável pelo tratamento ainda que de forma sumária, fazendo assim prova da sua efetiva realização. O responsável pelo tratamento poderá também ter necessidade de intervir diretamente no seu sistema (LMS), se dele depender assegurar que o aluno tem instalada a última versão da solução adotada para realização da prova. Não faria sentido que, por um lado se corrigissem os problemas de segurança encontrados e que, por outro, se continuasse a permitir a utilização de versões obsoletas e inseguras[85].

A comercialização no mercado negro, de soluções 'chave na mão' para aceder remotamente a dispositivos vulneráveis é uma realidade[86] atual, sendo inclusive utilizada por instituições governamentais de vários países.

Durante o processo de avaliação da necessidade de realização de uma AIPD, deve igualmente ter-se em conta as cláusulas contratuais associadas à prestação de serviços e às políticas de utilização dos mesmos. Embora muito se louve a iniciativa da FCT em disponibilizar a solução Colibri para coadjuvar, primeiro, o ensino a distância, e mais tarde a realização de provas de avaliação, não pode deixar de aqui se referir que poderia a mesma ter ido mais além na definição contratual dos já aqui referidos 'Termos de Utilização' do Colibri/Zoom,

[85] Falhas de segurança detetadas no Google Chrome (2650 milhões de utilizadores) e Zoom: <*https://www.wired.co.uk/article/google-chrome-windows-zoom-critical-update*>, <*https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=+Google+Chrome*>, <*https://explore.zoom.us/en/trust/security/security-bulletin*>.

[86] PERLROTH, Nicole, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race,* Bloomsbury Publishing, 2021.

destacando-se, desta vez, a secção 15 relativa à 'Ausência de Garantias'[87] e a secção 17, relativa 'Limitação de Responsabilidade'[88], das quais resultam abstratas garantias para os utilizadores finais do serviço – alunos e docentes –, mas também para as instituições de ensino enquanto responsáveis pelo tratamento dos dados.

Recorde-se, ainda, que nos casos em que não é clara a necessidade de realização de uma AIPD, o Grupo de Trabalho do art.º 29 recomenda a sua realização[89].

5.2. Tratamento de dados no processo de monitorização automática

Se nos modelos de monitorização anteriormente referidos se admite a discussão da obrigatoriedade de realização de AIPD, não parece que o mesmo se aplique aos tratamentos de dados sob o processo de monitorização automática. Independentemente de determinada solução dispor de um maior ou menor número de funcionalidades, a utilização de novas tecnologias[90], *prima facie*, será suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados.

---

[87] De onde se retira: "(…) a utilização dos serviços é exclusivamente por sua conta e risco. Qualquer material e/ou dados baixados ou de outra forma obtidos pela utilização dos serviços são por seu próprio critério e risco. Você será o único responsável por qualquer dano que possa decorrer da utilização dos serviços. Todo o risco decorrente da utilização ou desempenho dos serviços recai sobre você. A Zoom não assume qualquer responsabilidade pela retenção de qualquer informação de usuário ou comunicação entre usuários. A Zoom não pode garantir e não promete qualquer resultado específico da utilização dos serviços. A utilização é por seu próprio risco.", cf. consulta em 4 de fevereiro de 2023, (em linha) disponível em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*>.

[88] De onde se retira "Na extensão máxima permitida pela lei aplicável, em nenhum caso a Zoom ou suas afiliadas, fornecedores ou revendedores serão responsáveis por quaisquer danos especiais, incidentais, indiretos, punitivos ou consequenciais (…)", terminando do seguinte modo "Como alguns estados e jurisdições não permitem a exclusão ou limitação de responsabilidade, a limitação acima pode não se aplicar a você.". Disponível em: <*https://ajuda.colibri.fccn.pt/condicoes-de-uso*>, [4 fev. 2023].

[89] Cf. (p.9 *in fine*) Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679. Disponível em: <*https://www.cnpd.pt/media/f0ide5i0/aipd_wp248rev-01_pt.pdf*>.

[90] Cf. n.º 1 do art.º 35.º do RGPD.

Poderia essa avaliação estar dispensada, caso se verificasse uma das exceções previstas pelo n.º 5, ou pelo n.º 10, do art.º 35.º do RGPD. No entanto, estando implicado o tratamento de categorias especiais de dados pessoais, automaticamente se exclui o n.º 10, já que o mesmo incide sobre específicos fundamentos de licitude previstos no n.º 1 do art.º 6, e não no n.º 2 do art.º 9.º, conforme seria necessário para levantar a proibição daquele tratamento.

Por outro lado, pelo facto de não ter a CNPD publicado a lista (opcional) a que se refere o n.º 5 do art.º 35.º, relativa aos tipos de operações de tratamento para os quais não é obrigatória a realização de uma AIPD, se exclui também eventual exceção que ali pudesse estar prevista e ser aplicável ao caso em análise.

A utilização de soluções de monitorização automática, das quais resulte uma decisão de anular uma prova de avaliação tendo por base um tratamento automatizado, com recurso a definição de perfis, sempre obrigaria à realização de AIPD de acordo com a alínea *a)* do n.º 3 do art.º 35.º do RGPD. Mas, ainda que assim não se entendesse, ou se a decisão final de anular um exame fosse delegada no respetivo docente, após a sua análise, haveria que consultar a lista a que se refere o n.º 4 do art.º 35.º do RGPD, relativa aos tratamentos de dados pessoais sujeitos à realização de AIPD[91] e que se materializa no Regulamento 798/2018. Da sua análise e apreciação dos números 2, 5, 7 e 9 resultaria a clarividência da necessidade de realização de AIPD.

Tendo em conta a reflexão efetuada, resumem-se, de seguida, para cada uma das categorias de monitorização, os fundamentos de licitude adequados ao tratamento de dados e a necessidade de se realizar uma AIPD.

[91] Aprovada pelo Regulamento 798/2018, disponível em: <*https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121818*>.

Soluções de Monitorização	Fundamentos de licitude admissíveis	AIPD
Em tempo real	Alínea *a)* ou *e)* do n.º 1 do art.º 6.º do RGPD *(com as devidas anotações)* Ou Alínea *f)* do n.º 1 do art.º 6.º do RGPD *(se em causa estiverem instituições privadas)*	Recomendada
Recurso a gravação	*idem*	*idem*
Automática	Alínea *e)* do n.º 1 do art.º 6.º do RGPD, conjugada com a alínea *g)* do n.º 2 do art.º 9.º do mesmo diploma *(com as devidas anotações)* Ou Alínea *a)* do n.º 1 do art.º 6.º do RGPD, conjugada com a alínea *a)* do n.º 2 do art.º 9.º do mesmo diploma *(com as devidas anotações)*	Obrigatória

Tabela 2 – Relação dos fundamentos de licitude elegíveis e necessidade de realizar AIPD, consoante o tipo de monitorização

6. Conclusão

De forma geral, considera-se escassa a informação disponibilizada, nos sítios *web* das soluções comerciais, que contribua de forma útil para a perceção integral do respetivo modelo de funcionamento e dos dados suscetíveis de serem tratados. Tal facto não favorece nem as instituições de ensino, no momento da procura por soluções capazes de responder às suas necessidades, nem a tranquilidade dos alunos, quando procuram

informação após se verem confrontados com a necessidade de utilizar uma determinada solução comercial.

Realça-se, assim, a especial importância em disponibilizar, de forma pública ou reservada (*e.g.* restrita à comunidade académica visada), integral ou parcialmente, a AIPD que o responsável pelo tratamento tenha eventualmente realizado.

Ademais, determinadas soluções de monitorização possuem uma variedade de funcionalidades, cuja a opção pela sua utilização fará variar o grau de ingerência nos direitos e liberdades dos titulares dos dados. Nessa medida, têm as instituições de ensino, enquanto responsável pelo tratamento, a obrigação de verificar e demonstrar que o tratamento de dados pessoais que realizam, respeita os princípios e as regras legalmente aplicáveis, em matéria de proteção dos dados[92].

Por outro lado, apesar de se terrem elencado os possíveis fundamentos de licitude, para o tratamento de dados prosseguido por cada uma das três categorias de monitorização, compete a cada instituição de ensino avaliar e demonstrar que o concreto tratamento é, de facto, necessário, por não existirem, ou não serem efetivamente viáveis, outros métodos de avaliação menos intrusivos da privacidade dos titulares dos dados. Tal, aplica-se, não só na prossecução dos interesses (públicos) da instituição de ensino, mas também nas situações em que o titular dá o seu consentimento para tratamento dos seus dados.

Em suma, e de acordo com as Orientações da CNPD[93], "importa avaliar o tratamento à luz dos princípios da minimização dos dados pessoais e da proporcionalidade, nas vertentes da adequação, necessidade e proibição do excesso[94]". Não seria, portanto, razoável que, por via do recurso à monitorização da avaliação a distância, pretendesse o responsável pelo tratamento assegurar adicionais garantias, face às observadas no regime de avaliação presencial.

---

[92] Nos termos do n.º 2 do art.º 5.º e n.º 1 do art.º 24.º, ambos do RGPD.

[93] "Orientações sobre avaliação à distância nos estabelecimentos de ensino superior" (p.4, *in fine*), disponível em: <*https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf*>.

[94] Cf. alínea *c)* do n.º 1 do art.º 5.º do RGPD.

Nesse sentido, a monitorização em tempo real (sem gravação de áudio ou vídeo) parece ser o modelo que mais se aproxima da vigilância em regime presencial e, ainda, aquele que representa menor risco de ingerência nos direitos e liberdades dos titulares. A sua combinação com uma ferramenta de características semelhantes às que são conferidas pelo SEB, que é também de código aberto e por esse motivo mais transparente, é uma possibilidade indubitavelmente menos intrusiva face às soluções de monitorização automática. Por outro lado, permite igualmente o emparelhamento de um dispositivo secundário, que possibilita a captação, de outra perspetiva, do local em que o aluno realiza o exame, perfilando-se como alternativa adequada à captação de som.

O responsável pelo tratamento tem, de facto, uma panóplia de opções e efetiva liberdade de escolha, permitindo-lhe configurar um ambiente fiável para efeitos de avaliação a distância, em função das suas reais necessidades e do respeito pela privacidade dos titulares dos dados.