INSTITUTO
UNIVERSITÁRIO
DE LISBOA

UNIVERSIDADE NOVA
DE LISBOA

Sistemas de avaliação à distância no ensino universitário: desafios de conformidade com o RGPD

Saul André Nogueira Ferreira Leite

Mestrado em Engenharia de Telecomunicações e Informática,

Orientador:
Doutor Nuno Manuel Mendes Cruz David, Professor Associado,
Iscte - Instituto Universitário de Lisboa

Co-Orientador:
Doutor Francisco Pereira Coutinho, Professor Associado com Agregação,
Universidade NOVA de Lisboa

novembro, 2022

Departamento de Ciências e Tecnologias da Informação

Sistemas de avaliação à distância no ensino universitário: desafios de conformidade com o RGPD

Saul André Nogueira Ferreira Leite

Mestrado em Engenharia de Telecomunicações e Informática,

Orientador:
Doutor Nuno Manuel Mendes Cruz David, Professor Associado,
Iscte - Instituto Universitário de Lisboa

Co-Orientador:
Doutor Francisco Pereira Coutinho, Professor Associado com Agregação,
Universidade NOVA de Lisboa

novembro, 2022

“Mudam-se os tempos, mudam-se as vontades,

Muda-se o ser, muda-se a confiança”

Luís Vaz de Camões

Agradecimento

Agradeço ao meu Orientador Professor Doutor Nuno David e Co-Orientador Professor Doutor Francisco Pereira Coutinho, por terem abraçado este projeto desde o primeiro instante, pelas suas opiniões críticas e generosidade.

Agradeço a todos os que contribuíram para que levasse este estudo a bom porto, ao Engenheiro Jorge Ribeiro pelo apoio e motivação transmitidos, à Dra. Isabel Cruz e Dra. Clara Guerra pelos contributos e disponibilidade, à Professora Doutora Filipa Calvão pelo cuidado e atenção dispensada.

Por último, não menos importante, agradeço todo o carinho da minha família, a paciência e o apoio incondicional da minha noiva.

Resumo

A supervisão tradicional, conceptualmente humana, da avaliação de conhecimentos no ensino superior português, assegura a vigilância presencial dos avaliados e do meio envolvente, para que o processo de avaliação decorra sem sobressaltos.

É um processo de inquestionável maturidade, seja por via do enraizamento cultural, ou pela eficácia comprovada, revelando-se, ainda, um processo prático e adequado às suas finalidades.

O contributo dos avanços na área das novas tecnologias, aliado à particular situação de isolamento social a que nos conduziu a pandemia por COVID-19, revelaram-se condições propícias ao desejo de, em alguns casos, testar, e em outros colocar em prática, um sistema de avaliação à distância que permitisse, simultaneamente, vigiar os alunos e o ambiente de realização de uma prova.

Ultrapassada a urgência em alcançar uma solução, a que o tempo e a evolução favorável das condições sanitárias viriam a dar resposta, importará agora analisar as soluções de monitorização atualmente disponíveis e as técnicas computacionais a que recorrem, como a de Inteligência Artificial para tratamento de dados, incluindo dados biométricos, refletindo acerca do fundamento de licitude da sua utilização.

Vigorando atualmente o Regulamento Geral de Proteção de Dados (RGPD), pretende-se, igualmente, identificar em que condições a utilização destas ferramentas respeitará as disposições legais ali previstas.

Por fim, concluir-se-á que a obtenção do consentimento do utilizador será o meio que confere melhores garantias de um tratamento de dados pessoais lícito, incluindo de categorias especiais, simultaneamente em respeito pelos interesses, direitos e liberdades fundamentais do titular.

Palavras chave: RGPD; monitorização; avaliação à distância; ensino superior.

Abstract

The traditional proctoring process carried out at the Portuguese Universities has been implemented for several years, through human face-to-face interaction. In this process, the proctor guarantees the appropriate surveillance, ensuring the identity of the test taker and the integrity of the test-taking environment, intervening only whenever necessary, so that the evaluation process can run as smoothly as possible.

It has been a process of unquestionable maturity, either because of its cultural roots, or by the already demonstrated effectiveness over time, proving to be practical and adequate to its purposes. The development of new technologies, together with the particular situation of social isolation induced by the COVID-19 pandemics created the opportunity to test, in some cases, or even to use, remote proctoring systems to monitor the students and their environment, during their knowledge exams.

It is now important to analyze the available e-proctoring tools, and the associated technologies, including the use of artificial intelligence to process personal data, which can be biometric data, while assessing their lawfulness in the context of university exams.

Having regard to the General Data Protection Regulation (GDPR), currently in force, we propose to identify in what conditions the use of such tools would comply with the legal provisions. Finally, we conclude that obtaining the user's consent will be the best way to ensure a lawful processing of personal data, in particular of special categories of data, while guaranteeing data subject' interests, rights and fundamental freedoms.

Keywords: GDPR; proctoring; remote assessment; higher education.

Índice

Glossário

A3ES – Agência de Avaliação e Acreditação do Ensino Superior

AIPD – Avaliação de Impacto sobre a Proteção de Dados

CEPD – Comité Europeu para a Proteção de Dados, o mesmo que EDPB

Cf. – Confrontar

CNPD – Comissão Nacional de Proteção de Dados

DL – Decreto-Lei

e.g. – do latim, *exempli gratia* (por exemplo)

EDPB – *European Data Protection Board*, o mesmo que CEPD

ePrivacy – Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002

et al. – do latim, *et alii* (e outros)

EUA – Estados Unidos da América

FCCN – Unidade FCT – Unidade de Computação Científica da FCT

FCT – Fundação para a Ciência e a Tecnologia

FISA – *Foreign Intelligence Surveillance Act*

GPS – *Global Positioning System*

i.e. – do latim, *id est* (isto é)

IA – Inteligência Artificial

ibid. – *ibidem* (na/da mesma obra)

IES – Instituições de Ensino Superior

ITU – Universidade de Tecnologias de Informação de Copenhaga (*IT-Universitetet i København*)

OCDE – Organização para a Cooperação e Desenvolvimento Económico

RCTS – Rede Ciência, Tecnologia e Sociedade

RFID – *Radio-frequency Identification*

RGPD – Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) n.º 679/2016, de 27 de abril) e consequentes retificações

SAR – Sistemas de Avaliação Remota

TJUE – Tribunal de Justiça da União Europeia

UE – União Europeia

UvA – Universidade de Amesterdão (*Universiteit van Amsterdam*)

WP29 – *Article 29 Working Party* (Grupo de trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais)

CAPÍTULO 1

Introdução

O recurso às tecnologias de informação e comunicação para o apoio à atividade das instituições de ensino superior (IES) tem, ao longo dos anos, demonstrado proveitosos resultados designadamente em termos de: inclusão social do público alvo, sobretudo provenientes de zonas remotas; diversidade da oferta formativa e globalização do seu corpo docente; disponibilização constante e acesso imediato a recursos didáticos de qualidade.

Adaptada a sociedade à evolução permanente das novas tecnologias, a comunidade académica global e em particular aqueles que nos últimos anos procuraram obter competências específicas por via de certificação profissional, assistiram, particularmente, àquela que foi a tendência natural de introdução de novas formas de avaliação com recurso às tecnologias, em regime parcial[1] ou totalmente *online*[2].

O advento das soluções informáticas que, durante um processo de avaliação de conhecimentos à distância, se propõem à monitorização da conduta dos avaliados, e em certos casos, também da validação da sua identidade, viu nos tempos atípicos cunhados pela pandemia por COVID-19, a expectável oportunidade de expansão global e conquista de novos clientes. Tal frenesim, manifestou-se não só na quantidade de soluções emergentes, como pela disputa entre si na implementação de novas funcionalidades e modelos de licenciamento. E, se a integração com as plataformas de partilha de recursos, tão bem conhecidas das IES (*e.g. Blackboard, Moodle*), é já uma característica comum à maioria das atuais soluções, a aposta parece voltar-se agora para os métodos de *machine learning* e redes neuronais artificiais (*neural networks*), ou a aquisição a terceiros de serviços de inteligência artificial (IA) enquanto produto final, na expectativa de conferir ao processo de vigilância a robustez e credibilidade necessárias à deteção de fraude académica, desmaterializando o processo da intervenção humana.

Em março de 2020, impostas em Portugal as situações de confinamento e de isolamento social, veio o Decreto-Lei n.º 10-A/2020, de 13 de março, decretar a suspensão das atividades letivas e não

[1] Em 2015, a Pearson VUE, enquanto centro intermediário para a certificação de formação de entidades como Microsoft, IBM, ou Oracle, adquiriu a ProctorCam, uma ferramenta para monitorização de avaliações à distância, como forma de complemento à vigilância presencial que era já conferida nos centros de avaliação [1]. Em 2019, a mesma empresa acabaria por disponibilizar uma solução (OnVUE) para monitorização da avaliação de conhecimentos, em regime totalmente *online* [2].

[2] Em 2020, a universidade McGraw-Hill anunciou a celebração de uma parceria para a integração da ferramenta Proctorio na sua plataforma digital de ensino (McGraw-Hill Connect), como solução para a realização de avaliação de conhecimentos à distância [3].

letivas presenciais nos estabelecimentos de ensino superior. Esse facto, dificilmente expectável em período pré-pandemia, impôs que os referidos estabelecimentos repensassem, em tempo recorde, os canais de comunicação mais adequados a diversas finalidades, entre as quais se encontraria presumivelmente a de realização das atividades de avaliação contínua e/ou final dos estudantes.

O artigo 6.º do DL n.º 20-H/2020, de 14 de maio, com efeitos ao dia seguinte da sua publicação, derrogou, contudo, a suspensão das atividades letivas e não letivas presenciais. Nesse sentido, as recomendações[3] do Ministério da Ciência, Tecnologia e Ensino Superior admitiam a menor adequação de processos à distância, designadamente o de avaliação final dos estudantes. De igual importância se revelaram as posteriores orientações da Comissão Nacional de Proteção de Dados (CNPD) [6], acerca da avaliação à distância nos estabelecimentos de ensino superior, preventivas, mas não impeditivas, e em tudo em linha com as suas anteriores orientações para utilização de tecnologias de suporte ao ensino à distância [7].

No entanto, as IES foram definindo estratégias de avaliação à distância, em alguns casos, chegando a adquirir soluções integradas para esse fim, abandonando-as mais tarde, fosse por dúvidas quanto à licitude do tratamento dos dados, fosse pela natureza das aplicações frequentemente descritas de forma vaga, gerando dúvidas quanto à sua conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD).

A este propósito, a Fundação para a Ciência e a Tecnologia (FCT), através da Unidade de Computação Científica (FCCN), iniciou, em abril de 2020, um piloto de sistemas de avaliação à distância junto da comunidade académica – Piloto SAR – que viria a terminar em julho do mesmo ano, de acordo com a duração prevista [8]. O projeto visou a disponibilização de quatro soluções comerciais[4] de monitorização da avaliação à distância, posteriormente disponibilizadas aos docentes da comunidade académica conectada à RCTS, para efeitos de avaliação das plataformas [9]. Do referido projeto foi possível concluir, essencialmente, que as soluções de mercado, em especial as soluções 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. Apesar dos elevados custos de licenciamento e das complexidades legais associadas à incerteza ou falta de transparência no que respeita à forma de tratamento, períodos de retenção e destino dos dados pessoais, a totalidade dos participantes manifestou interesse em que fosse encontrada uma solução que se proponha às mesmas finalidades, cumprindo com os requisitos identificados [8],[9],[10].

[3] "Recomendação às instituições científicas e de ensino superior relativamente à cessação do estado de emergência motivado pela pandemia COVID-19", de 30 de abril de 2020 [4] e "Recomendação às instituições científicas e de ensino superior para garantir o processo de reativação faseada e responsável das atividades na presença de estudantes, docentes e investigadores", de 15 de maio de 2020 [5].

[4] ProctorExam, pela Universidade de Lisboa; TestWe pelo Instituto Politécnico de Bragança; Exam.net pela Universidade de Trás-os-Montes e Alto Douro; e Respondus pela Universidade de Aveiro.

Em maio de 2021, na sequência de uma queixa apresentada à CNPD, denunciando a intenção de uma instituição de ensino superior em recorrer à utilização de uma solução[5] para vigilância dos alunos, durante a avaliação à distância, após ter analisado o caso, a autoridade de proteção de dados advertiu o responsável pelo tratamento de que a utilização daquela solução (constituída por duas aplicações) era suscetível de violar os princípios da licitude, finalidade, proporcionalidade e da minimização dos dados pessoais dos alunos. Ordenou, ainda, para que desse de imediato instruções ao subcontratante para a destruição de todos os dados recolhidos quanto aos alunos que haviam já instalado as aplicações nos seus dispositivos. No seu Parecer [11], a CNPD começa por criticar a falta de definição de circunstâncias específicas ou critérios ponderosos que justifiquem o uso da solução, encontrando-se delegada essa responsabilidade, por despacho reitoral, nos coordenadores das respetivas unidades curriculares. Levanta dúvidas quanto ao fundamento de licitude invocado para o tratamento dos dados, baseado no interesse legítimo do responsável pelo tratamento, quando aquela instituição tem por missão manifestamente a prossecução do interesse público, admitindo que mesmo que assim não se entendesse, teria sempre que haver lugar a um exercício de ponderação da prevalência dos interesses ou direitos e liberdades fundamentais dos titulares dos dados, o que não se verificou. Apesar da instituição ter efetuado uma avaliação de impacto sobre a proteção de dados (AIPD), considerou a autoridade que as medidas identificadas para mitigação dos riscos pecavam por defeito, sendo desadequadas à dimensão e extensão do tratamento. Em especial, referiu que a instituição de ensino aceitou que a empresa subcontratada recolhesse gravações de áudio e vídeo dos estudantes, não só no contexto de prestação do serviço, mas também para os seus próprios fins, para investigação e melhoria do seu produto. Do mesmo contrato, resultaria ainda a transferência dos dados pessoais para um país que, como iremos ver mais à frente, não permite que seja garantido um nível de proteção de dados equivalente ao da UE.

À semelhança de Portugal, verificou-se a nível europeu uma série de acontecimentos que corroboram os exigentes desafios na observância e cumprimento das disposições legais, especialmente em matéria de proteção de dados pessoais. Num dos casos, a autoridade de proteção de dados italiana (*Garante per la protezione dei dati personali*) aplicou, em 16 de setembro de 2021, uma coima no valor de 200.000 euros à Universidade *Luigi Bocconi*, em Milão. Na origem da decisão [12] esteve a utilização de um sistema de monitorização dos alunos, durante a avaliação à distância que, pelas suas características, e pelo modo como a Universidade realizou o tratamento de dados, resultou na violação de princípios relativos ao tratamento de dados pessoais: licitude, lealdade e transparência; minimização dos dados; e limitação da conservação. Verificou-se, ainda, não estarem reunidas as condições de licitude para o tratamento de dados, incluindo de categorias especiais; falta

[5] Respondus, constituída pelas ferramentas 'Lockdown Browser' e 'Respondus Monitor'.

de informação aos titulares dos dados; não observância da proteção dos dados desde a conceção e por defeito; falta de indicação de medidas apropriadas à mitigação dos riscos, na AIPD; e violação do princípio geral das transferências (artigo 44.º e Considerandos 101 e 102, todos do RGPD).

Por sua vez, a Autoridade de proteção de dados dinamarquesa (*Datatilsynet*), numa decisão de 26 de janeiro de 2021 [13], na sequência da inspeção por si realizada em 30 de abril de 2020, decidiu a favor da Universidade de Tecnologias de Informação de Copenhaga (ITU), em virtude da mesma se ter socorrido de um software[6] para monitorização dos alunos no processo de avaliação à distância. Fundamentou a Autoridade que a Universidade foi instruída pelas autoridades dinamarquesas para que, face ao contexto de pandemia por COVID-19, prosseguisse o ensino e as respetivas avaliações em regime *online*. Na sua análise, entendeu, ainda, que a Universidade fez uma avaliação correta e documentada da necessidade de utilização da ferramenta de monitorização; escolheu a ferramenta menos intrusiva, face às circunstâncias, tendo informando devidamente os alunos sobre o tratamento extraordinário de dados, que considerou lícito nos termos da alínea e) do n.º 1 do artigo 6.º do RGPD. Verificou, ainda, que a Universidade realizou a AIPD, adotando as medidas de segurança técnicas e organizativas adequadas, em cumprimento do RGPD e da lei nacional de proteção de dados. No entanto, a autoridade de proteção de dados não se pronunciou quanto à transferência de dados para os EUA[7].

Num caso holandês [14] que remonta a factos ocorridos em maio de 2020, o Tribunal de Primeira Instância de Amsterdão deu razão à Universidade de Amsterdão (UvA), numa consulta preliminar que lhe foi dirigida por um estudante e representantes de um grupo de estudantes daquele estabelecimento de ensino superior. Entendeu o Tribunal que, face às medidas à altura em vigor e que determinaram a suspensão das atividades de ensino e de avaliação presenciais, devido à pandemia por COVID-19, a utilização de software de vigilância[8] foi uma alternativa adequada, considerando igualmente válido o fundamento de licitude do tratamento de dados, para efeito dos interesses legítimos do responsável pelo tratamento. Concluiu, ainda, que gravar imagens via *webcam* do aluno e do espaço que o rodeia não constitui um tratamento de categorias especiais de dados pessoais, porquanto não serem tratados dados biométricos ou relativos ao movimento dos olhos, da respiração ou stresse, tendo sido respeitados os princípios relativos ao tratamento de dados, previstos no RGPD.

[6] ProctorExam, que solicitava (via *webcam*) a exibição do documento de identificação ou cartão de estudante, posteriormente verificado por funcionário da ITU. Gravava o histórico do browser *web*, som e imagem da *webcam* e do monitor do aluno. Não havia lugar a tratamento de dados biométricos, nem eram usadas tecnologias de reconhecimento facial.

[7] No ponto 4.2 do Capítulo 4.º, é abordada a invalidação do acordo *Privacy Shield*, que até então legitimava a transferência de dados pessoais entre os países da UE e os EUA.

[8] Proctorio, que procede à gravação de imagens via *webcam*, áudio, tráfego e dados de *input*. Apesar do software suportar deteção facial, o Tribunal refere que não foram usados dados biométricos.

Face ao exposto, pretende-se verificar em que condições se poderá, legalmente, recorrer a sistemas de monitorização da avaliação à distância no ensino superior, e em que medida poderão as ferramentas utilizar dados biométricos na busca da eficácia e confiança desejáveis, para a dissuasão e deteção de práticas suscetíveis de constituírem fraude académica.

Relativamente aos dados biométricos, será analisado o seu conceito, clarificando-se as restrições e as condições necessárias ao seu tratamento.

O presente estudo é composto por cinco capítulos, correspondendo o primeiro e atual capítulo aos aspetos verificados e que motivaram a realização do estudo. O capítulo segundo, relativo ao regime jurídico da proteção de dados pessoais, aborda disposições legais aplicáveis e os meios de verificação da sua aplicação, os principais conceitos e princípios relativos ao tratamento e à proteção de dados pessoais, exemplificando-se a sua importância através de um exemplo prático. O capítulo terceiro apresenta uma proposta de categorização das ferramentas de monitorização do processo de avaliação à distância, atendendo aos recursos necessários e às técnicas aplicadas por cada uma, descrevendo-se, ainda, para familiarização do leitor, as funcionalidades das atuais soluções comerciais. No capítulo quarto são analisadas as particularidades a observar no tratamento de dados biométricos, enquanto categoria especial de dados pessoais. Serão elencados os motivos e as consequências da invalidação, pelo TJUE, da Decisão 2016/1250, relativa à proteção fornecida pelo acordo UE-EUA para a transferência de dados pessoais, com impacto direto nos tratamentos que não assegurem um nível de proteção equivalente ao da UE. Por último, serão considerados os aspetos legais a observar na conceção e na utilização de algoritmos de Inteligência Artificial. O capítulo quinto reserva-se integralmente à apresentação das conclusões retiradas ao longo do estudo.

CAPÍTULO 2

Regime jurídico da proteção de dados

Para que melhor se compreenda a análise efetuada neste estudo, será relevante familiarizar o leitor os conceitos, princípios e considerandos do RGPD, contextualmente relevantes, o que se fará ao longo deste capítulo.

2.1. Regulamento Geral sobre a Proteção de Dados

O Regulamento Geral sobre a Proteção de Dados (vulgarmente e doravante designado por RGPD), é o Regulamento n.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. A sua execução na ordem jurídica nacional é assegurada pela Lei n.º 58/2019, de 8 de agosto, Lei da Proteção de Dados Pessoais.

A referida lei designa a Comissão Nacional de Proteção de Dados (CNPD), enquanto entidade administrativa independente dotada de autonomia administrativa e financeira, com poderes de autoridade para o controlo e fiscalização do cumprimento do RGPD e da referida Lei, e demais disposições legais e regulamentares, em matéria de proteção de dados pessoais.

Por sua vez, através da Deliberação 2019/494, de 3 de setembro [15], a CNPD decidiu desaplicar um conjunto de dez normas da Lei da Proteção de Dados Pessoais, por considerar que as mesmas violam o próprio RGPD. Passou, assim, a aplicar diretamente as normas do diploma da União, assegurando o primado do direito da União e a efetividade do RGPD [16].

Uma das normas desaplicadas pela CNPD é o n.º 1 do artigo 23.º, por admitir genericamente que o tratamento de dados pessoais por entidades públicas possa ser realizado para finalidades diferentes das que justificam a recolha de dados, violando o princípio da limitação das finalidades, consagrado na alínea b) do n.º 1 do artigo 5.º, e o n.º 4 do artigo 6.º do RGPD, por não haver uma norma do direito nacional, ou da União, que fixe as tarefas e finalidades específicas que o tratamento ulterior vise prosseguir [15].

2.2. Principais conceitos relativos à proteção de dados pessoais

O artigo 4.º do RGPD define conceitos relativos aos dados pessoais e à sua proteção. Enumerar-se-ão, de seguida, aqueles que se consideram pertinentes para o presente estudo.

«Dados pessoais» a informação relativa a uma pessoa singular identificada ou identificável, «titular dos dados», sendo considerada uma pessoa singular identificável aquela que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (*eg.* nome, número de identificação), ou a um ou mais elementos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. De notar que há uma categoria especial de dados pessoais, que pelos especiais riscos que o seu tratamento importa, está sujeita a um regime reforçado de proteção. Os dados especiais são os elencados no n.º 1 do artigo 9.º do RGPD, e o seu tratamento depende de, desde logo, se verificar uma das condições previstas no n.º 2 do mesmo artigo.

Por «tratamento» entende-se a operação ou 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.

O «responsável pelo tratamento» 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.

O «consentimento» do titular dos dados é uma manifestação de vontade, livre, específica, informada e inequívoca[9], 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.

2.3. Princípios e considerações relativos ao tratamento de dados pessoais

O tratamento de dados pessoais deverá obedecer ao cumprimento dos princípios definidos no artigo 5.º do RGPD, prevendo este que os dados pessoais sejam objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);

Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades («limitação das finalidades»);

Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

Exatos e atualizados sempre que necessário; devem 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 («exatidão»);

[9] A segunda retificação ao Regulamento Geral sobre a Proteção de Dados, publicada no jornal oficial da União a 4 de março de 2021, substituiu a expressão «explícita» por «inequívoca» [17].

Conservados de forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados («limitação da conservação»);

Tratados de forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).

O responsável pelo tratamento é responsável direto pelo cumprimento dos princípios anteriores, estando sujeito ao dever de o comprovar («responsabilidade»).

2.4. Proteção de dados desde a conceção e por defeito

A implementação de medidas para assegurar a proteção dos dados era tipicamente um aspeto secundário, a pensar *a posteriori*, muitas vezes já adquirida a solução para o tratamento dos dados pessoais [18]. O RGPD extrapolou regras estabelecidas pela Diretiva de Proteção de Dados Pessoais n.º 95/46/CE (revogada pelo RGPD), atualizando não só requisitos e princípios, mas também, introduzindo novos conceitos, designadamente o da pseudonimização, e novas obrigações, nomeadamente a de implementação da proteção dos dados desde a conceção e por defeito [19]. Para a ideia atualmente subjacente a estes últimos conceitos, contribuiu a referida Diretiva, ao prever a adoção de medidas técnicas e organizativas adequadas, aquando da conceção dos sistemas e durante o tratamento de dados pessoais, impedindo tratamentos não autorizados. Contribuíram, também, os estudos de Ann Cavoukian [20], em 2010, com a definição de sete princípios fundamentais[10], em linha com os atuais princípios relativos ao tratamento de dados pessoais do RGDP. Contribuíram, ainda, os estudos pertinentes e visionários prosseguidos pela OCDE [21], [22] e o compromisso assumido [23], no mesmo ano, pela Conferência Internacional de Comissários de Proteção de Dados e de Privacidade (ICDPPC)[11], para: o reconhecimento e o acompanhamento da temática enquanto componente essencial aos fundamentos de proteção dos dados; a adoção de princípios, como os definidos por Cavoukian, nas orientações das respetivas autoridades de proteção de dados; e a sua divulgação junto da comunidade e do respetivo legislador nacional.

[10] *Proactive not Reactive; Preventative not Remedial*
Privacy as the Default
Privacy Embedded into Design
Full Functionality: Positive-Sum, not Zero-Sum
End-to-End Lifecycle Protection
Visibility and Transparency
Respect for User Privacy

[11] Fórum de alcance global das Autoridades de proteção de dados e de privacidade, que se reuniram pela primeira vez em Bona, na Alemanha, em 1979. Após 2019 adotou a designação de Assembleia Mundial da Privacidade – GPA (Global Privacy Assembly). Congrega atualmente mais de 130 autoridades de todos os continentes e vários observadores.

2.4.1. Proteção de dados desde a conceção

Com o RGPD, foi reforçado o conceito de proteção de dados desde a conceção, ao assegurar-se, através do n.º 1 do Artigo 25.º, que o responsável pelo tratamento dos dados (não diretamente o subcontratante) tem em conta a proteção de dados dos titulares desde o primeiro momento, tanto na definição dos meios de tratamento como durante o próprio tratamento dos dados. Para tanto, deve atender aos seguintes aspetos: as técnicas mais avançadas[12]; os custos da sua aplicação; a natureza do tratamento dos dados; o seu âmbito; o respetivo contexto; as respetivas finalidades; e os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem variar.

2.4.2. Proteção de dados por defeito

É a resposta à prática comum da recolha e tratamento do maior número possível de dados pessoais, ainda que sem necessidade para as finalidades prosseguidas. O âmbito de aplicação encontra relação direta com princípios relativos ao tratamento de dados pessoais e diz respeito: à quantidade de dados pessoais recolhidos (minimização dos dados); à extensão do seu tratamento (limitação das finalidades); ao prazo da sua conservação (limitação da conservação); e a sua acessibilidade. Relativamente ao termo 'acessibilidade', não se encontrando relação direta com qualquer um dos princípios relativos ao tratamento de dados, vem o ponto 55 da Diretriz n.º 4/2019 do CEPD [24], esclarecer que o alcance do termo tem o propósito dual de limitar as pessoas que podem aceder aos dados, com base numa avaliação da necessidade, garantindo igualmente que os dados pessoais estão acessíveis a quem deles necessita quando necessário (disponibilidade), devendo o acesso ser monitorizado. Parece-nos, assim, ir ao encontro do princípio da integridade e confidencialidade.

Aplica-se diretamente ao responsável pelo tratamento e indiretamente ao subcontratante, já que nos termos do n.º 1 do Artigo 28.º do RGPD, o primeiro apenas recorre ao segundo caso este apresente garantias suficientes da execução de medidas técnicas e organizativas adequadas, de uma forma que o tratamento satisfaça os requisitos do Regulamento e assegure a defesa dos direitos dos titulares dos dados.

2.4.3. Aplicabilidade em contexto prático

Pese embora com significados distintos, os conceitos de proteção de dados desde a conceção e de proteção de dados por defeito relacionam-se entre si.

[12] Na versão inglesa "*state of the art*", correspondendo às possibilidades tecnológicas científica e tecnicamente demonstradas [15].

Proteção de dados desde a conceção refere-se à conceção e existência de medidas e de mecanismos de segurança integrados que protegem o direito à proteção dos dados, durante o ciclo de vida da aplicação, serviço, ou produto [19].

Proteção de dados por defeito refere-se à implementação, por omissão, das medidas e mecanismos anteriormente referidos [25], *i.e.*, na configuração por omissão, o utilizador (titular dos dados) encontra-se já protegido [26].

Veja-se, a título de exemplo, o caso prático que se apresentará de seguida, com aplicação direta em algumas soluções de avaliação à distância. Um navegador web (*web browser*) pode, de forma automática, reduzir a sua 'pegada' (*browser fingerprint*), ao implementar opções que contribuam para a proteção dos dados do utilizador, tais como: envio do campo DNT[13] com o valor '1', no pedido da página; eliminar automaticamente o histórico de navegação, testemunhos de conexão e armazenamento local do navegador (*local storage*), ao fechar a sessão; desabilitar o *javascript*; entre outros [28], [29]. O desenvolvimento (conceção) e a integração de tais mecanismos estão diretamente relacionados com a proteção de dados desde a conceção. No entanto, a mera existência de tais opções não determina a verificação do princípio da proteção dos dados por defeito, a menos que tais opções sejam ativadas por omissão. Nesse sentido, a proteção dos dados por defeito depende da proteção dos dados desde a conceção. No entanto, a proteção dos dados desde a conceção é independente da proteção dos dados por defeito [19].

Na prática e atendendo ao disposto no artigo 25.º do RGPD, ambos os princípios constituem obrigações legais, cabendo ao responsável pelo tratamento verificar o seu cumprimento.

[13] DNT (*Do Not Track*) [27] é um campo do cabeçalho HTTP (*Hypertext Transfer Protocol*, usado no pedido de páginas *web*), que ao ser enviado com o valor '1' informa o servidor, ao qual foi solicitada a página *web*, que o utilizador não pretende ser rastreado. A sua utilização tem efeito prático muito residual, já que a sua implementação não é obrigatória. Por outro lado, esta lógica é contrária ao espírito do RGPD e da Diretiva ePrivacy (que aborda os testemunhos de conexão – *cookies)*, de onde se infere que o rastreamento do utilizador apenas é admissível após o seu consentimento, na acessão do seu significado, à luz do RGPD.

CAPÍTULO 3

Ferramentas de monitorização da avaliação à distância

3.1. Categorização das ferramentas

As ferramentas de monitorização à distância exploram, por via da ligação à internet, os recursos e características do dispositivo utilizado para a realização da prova de avaliação, recorrendo à câmara (*webcam)* do dispositivo e, em certos casos, também ao microfone.

As ferramentas podem ser enquadradas nas seguintes categorias, sem prejuízo da possibilidade de combinação entre si [30] [31]:

I. Monitorização em tempo real, necessitando para tanto de um ou mais avaliadores remotamente ligados, nos quais é delegada a responsabilidade de verificação da identidade e de monitorização dos avaliados, prevenindo a adoção de comportamentos suscetíveis de configurar fraude, durante o período de realização da prova de avaliação;

II. Monitorização com recurso à gravação de vídeo, na qual se procede à gravação dos examinados durante a realização da prova de avaliação, sem outros intervenientes. As gravações são posteriormente analisadas por quem tenha essa função, podendo ser professores ou terceiros contratados para o efeito, na busca de eventuais indicadores da prática de fraude.

III. Monitorização automática, através da qual se gravam os comportamentos dos avaliados durante a prova de avaliação, sendo essas gravações automaticamente processadas por um sistema de análise de áudio e vídeo, para deteção e classificação de comportamentos suspeitos ou ilícitos.

3.2. Principais funcionalidades

Tendo por base o levantamento efetuado em 2021 por Arnò *et al.* [31], relativo às soluções comerciais[14] de monitorização do processo de avaliação à distância e respetivas funcionalidades, elencam-se de seguida as funcionalidades identificadas:

[14] Soluções comerciais consideradas no estudo: ProctorU, Proctortrack, ProctorExam, Respondus, RPNow, Proctorio, 110 Cum Laude, Examity, MettL, AIProctor, Smowl, ProctorCam, Honorlock, Safe Exam Browser, Tegrity, Proview, ExamSoft, Exam.net, Top Hat, SmarterProctoring, ProProctor, Kryterion, Inc., Loyalist Exam Services, QuestionMark, Take a Test, Oxagile, Comprobo, Proctor360, Kanpur project.

- Integração com sistemas de apoio ao ensino LMS (*learning management systems*), designadamente Moodle, Blackboard ou Canvas, permitindo através dos últimos a criação das provas de avaliação e a respetiva configuração de funcionamento da solução de monitorização (*eg.* gravar apenas vídeo, gravar áudio e vídeo, avisos prévios à gravação, solicitação de documento de identificação);
- Autenticação do avaliado através da verificação da sua identidade, geralmente por via da exibição do documento de identificação ou do cartão de estudante; validação do email ou do nome de utilizador e respetiva palavra-passe; ou ainda através do reconhecimento facial, voz, impressão digital, íris, padrão de escrita, ou outros dados biométricos.
- Suporte de dispositivo secundário Android/iOS, como complemento à monitorização do aluno e do espaço físico em que o mesmo se encontra.
- Confinamento ao navegador *web* (*browser lockdown*), que fica geralmente em modo de ecrã-inteiro, bloqueando certas funcionalidades, entre as quais a de abertura de novos separadores ou acesso a outras páginas *web*. De igual modo, são bloqueadas as funcionalidades de virtualização, de execução de aplicações externas, do copiar e colar, das opções do botão direito do rato, de fotografia de ecrã (*screenshot*) e impressão, procedendo-se ao registo de todo o tráfego web.
- Monitorização, através das funções de: gravação do meio envolvente; sinalização de comportamentos suspeitos, com referência ao instante temporal; tecnologia de inteligência artificial; gravação áudio; gravação do monitor do estudante; registo da utilização do microfone e *webcam*; análise dos movimentos da cabeça e dos olhos do estudante; revisão de comportamento suspeito detetado; análise de áudio em tempo real; limitação geográfica, por via de GPS ou RFID, aos locais admissíveis à realização do exame; e recurso a *webcam* secundária. Uma ferramenta[15] não incluída no referido levantamento transcreve os discursos detetados via microfone, recorrendo a um serviço de terceiros.
- Terminar automaticamente o exame, caso detete que o aluno adotou um comportamento classificado como fraudulento;
- Suporte à comunicação, em tempo real (*live chat*), entre docente e examinando;
- Escalabilidade da solução, através do dimensionamento da capacidade de responder rapidamente às solicitações. A escalabilidade dinâmica é sobretudo uma característica das soluções que assentam em computação na nuvem (*cloud computing)*.

[15] WISEflow.

Entre as soluções, destaca-se o facto de algumas requererem a instalação de uma aplicação no dispositivo do aluno, de um *plugin* no *web browser* (de entre os suportados), ou ambos. Em parte das soluções identificadas, esses requisitos são apenas compatíveis com alguns sistemas operativos: Windows, Mac OS e Linux para computadores; Android e iOS para dispositivos móveis.

Assinala-se ainda que algumas das soluções indicam como funcionalidade o facto de estarem de acordo com o RGPD, ainda que de forma geral não mencionem em que medida(s).

Existem soluções que oferecem monitorização em tempo real combinada com a monitorização automática, verificando continuamente a identidade do examinando, para detetar e dissuadir comportamentos suscetíveis de serem fraudulentos.

Parte das soluções recorrem a serviços de terceiros, designadamente para o alojamento e demais operações de tratamento dos dados (*eg. Amazon S3*, para alojamento; *Amazon EC2*, para computação/processamento; *Amazon Transcribe*, para reconhecimento de voz e conversão em texto).

Em geral, as soluções que oferecem monitorização automática assentam em computação na nuvem (*cloud computing*).

CAPÍTULO 4

Conformidade do tratamento

No momento da avaliação de conhecimentos em regime presencial, ocorre naturalmente um processo chave que consiste na verificação da identidade do aluno, podendo ser: à entrada da sala; durante a prova; no momento da sua entrega; ou uma qualquer combinação dos três cenários anteriores. Ora, este processo permite não só atestar que o examinando é quem alega ser, mas ainda, que o mesmo não é substituído por um terceiro, ao longo do tempo de duração da prova.

Pelo mesmo motivo, importa conferir iguais garantias ao processo de monitorização da avaliação à distância.

Tendo em conta não ser humanamente possível uma monitorização atenta e fiável, quando em causa estão dezenas ou centenas de alunos, a menos que se multipliquem também os examinadores, o que nem sempre é possível ou sinónimo de melhores garantias, foram várias as soluções comerciais que propuseram métodos alternativos de autenticação, por via do reconhecimento facial, não só para autenticação do aluno na admissão à sala virtual de exame, como também durante o seu período da sua realização.

Neste capítulo, pretende-se aferir em que condições, à luz do RGPD, poderão as IES recorrer às soluções comerciais que utilizam tecnologia de reconhecimento facial. Para o efeito, considerar-se-ão as condições de licitude do tratamento de dados pessoais, mas também as específicas condições exigidas para eventuais transferências internacionais de dados (atendendo, em particular, à circunstância de a maior parte das soluções comerciais, de monitorização do processo de avaliação, serem disponibilizados por empresas com sede nos Estados Unidos da América).

4.1. Tratamento de dados biométricos

O recurso a técnicas de reconhecimento facial com o objetivo de validar a identidade de um aluno, remete-nos para o conceito de dados biométricos à luz do RGPD:

> "«Dados biométricos», 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."[16]

De uma primeira análise ao n.º 1 do artigo 9.º do RGPD, entender-se-á que o tratamento de dados biométricos, só por si, não corresponde ao tratamento de categorias especiais[17] de dados pessoais, não sendo abrangidos pela proibição do seu tratamento, já que o artigo se refere especificamente a "dados biométricos para identificar uma pessoa de forma inequívoca".

Por outro lado, refere o considerando 51 do RGPD que "o tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular."

Por forma a esclarecer as dúvidas a que a interpretação das disposições possa conduzir, tomaremos por referência o Parecer 3/2012 do WP29[18], sobre a evolução das tecnologias biométricas [32], onde se distinguem dois conceitos (tradução livre):

> Identificação biométrica - a identificação de um indivíduo através de um sistema biométrico é geralmente um processo de comparação de dados biométricos desse indivíduo (adquiridos no momento da identificação) com uma série de *templates* biométricos armazenados numa base de dados (ou seja, um processo de comparação de um para muitos).
>
> Verificação/autenticação biométrica - a verificação de um indivíduo através de um sistema biométrico é geralmente o processo de comparação dos seus dados biométricos (adquiridos no momento da verificação) com um *template biométrico* único, armazenado num dispositivo (*i.e.*, um processo de comparação de um para um).

[16] Ponto 14 do artigo 4.º do RGPD

[17] De acordo com o n.º 1 do artigo 9.º do RGPD, dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

[18] Grupo de trabalho europeu, independente, previsto pelo artigo 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 grupo substituído pelo EDPB/CEPD.

Esta interpretação é consistente com a posição da Comissão Europeia, patente no Livro Branco sobre a inteligência artificial [33]:

> "Em relação ao reconhecimento facial, 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.";
>
> "Autenticação (ou verificação), por outro lado, é frequentemente designada por correspondência «um a um». Permite a comparação de dois modelos biométricos, que geralmente se pressupõe pertencerem à mesma pessoa. Os dois modelos biométricos são comparados para determinar se a pessoa que aparece nas duas imagens é a mesma. Este procedimento é utilizado, por exemplo, nas portas de embarque com controlo automatizado nas fronteiras (ABC) utilizadas para os controlos de fronteira nos aeroportos."

Assim, poderá sustentar-se que, de acordo com o artigo 4.º do RGPD, o conceito de dados biométricos abrange tanto a identificação, como a verificação/autenticação. Contudo, os dados biométricos devem ser considerados dados especiais, para o efeito do n.º 1 do artigo 9.º do RGPD, apenas nos casos em que sejam submetidos a um tratamento técnico para identificação biométrica (comparação de um para muitos), e não no caso de verificação/autenticação biométrica (comparação de um para um).

Ressalva-se, porém, que, atendendo à complexidade da questão e ao sentido interpretativo que lhe possa ser associado, deverá sempre ter-se em conta a especificidade do concreto caso, em função dos dados tratados e das técnicas utilizadas para o seu tratamento, bem como a interferência com o direito à proteção de dados que daí resulte. Em caso de dúvida deverá ser adotada a interpretação mais favorável à proteção dos direitos dos titulares, *i.e.*, considerar que em causa está o tratamento de dados pessoais especiais.

Atendendo à variedade de soluções de vigilância da avaliação à distância, e à dispersão de funcionalidades descritas no ponto 3.2 do capítulo terceiro, destacam-se, essencialmente, três vertentes:

i. Gravação de som e imagem, respetivamente, através de microfone e de *webcam e/*ou outro(s) dispositivo(s) secundário(s) como telemóvel ou *tablet*, com objetivo primário de captar imagens do aluno antes e durante o exame, mas também do meio que o rodeia.
ii. Acesso ao dispositivo do aluno, para bloqueio da execução de aplicações alheias ao sistema operativo e à aplicação utilizada para realizar e vigiar do exame; e para recolha de informação

relativa ao tráfego gerado e às interações do aluno com o dispositivo, durante a realização da prova.

iii. Processamento de dados biométricos, na identificação através de reconhecimento facial, ou no tratamento de dados relativos ao padrão de escrita (*keystroking*), comportamentos gestuais, respiração (incluindo suspiros), estados de espírito (preocupação, ansiedade, etc.), entre outros.

As soluções de monitorização que asseguram que terceiros não se substituem ao aluno a avaliar, tanto no momento inicial, como durante o processo avaliação de conhecimentos, recorrem à sua identificação por via de técnicas de reconhecimento facial, gravando e comparando os dados adquiridos, em diferentes instantes, com os dados biométricos previamente armazenados nos seus sistemas. Os dados biométricos aqui empregues deverão ser entendidos em sentido lato, já que aos primeiros se poderão associar os mencionados no anterior ponto iii., por forma a conferir eficiência ao algoritmo de identificação.

Assim, tendo em conta as situações específicas de tratamento de dados biométricos para identificação facial, não só num determinado instante, mas numa base contínua, e na qual se admite a possibilidade de comparação com dados biométricos de terceiros para aferir quanto à possibilidade de o aluno se ter feito substituir por um terceiro, somos a concluir que os processos de reconhecimento facial, nestes termos, envolvem o tratamento de dados biométricos para identificar uma pessoa de forma inequívoca.

Se dúvidas restassem, tome-se a posição do Comité Europeu para a Proteção de Dados[19] que, nas suas Diretrizes 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo [34], ao entender que a utilização de reconhecimento biométrico nos sistemas de videovigilância corresponde ao tratamento de uma categoria especial de dados:

> "A utilização da videovigilância, incluindo a funcionalidade de reconhecimento biométrico, instalada por entidades privadas para os seus próprios fins (por exemplo, comercialização, estatísticas ou até mesmo segurança) exigirá, na maioria dos casos, o consentimento explícito de todas os titulares dos dados (artigo 9.º, n.º 2, alínea a)), embora também possa ser aplicável outra exceção adequada prevista no artigo 9.º.",

Dando ainda o seguinte exemplo:

[19] CEPD/EDPB é o órgão independente da União Europeia que sucedeu ao WP29, com a aplicação do RGPD, tendo, entre outras missões, a de dar orientações gerais (incluindo diretrizes, recomendações e boas práticas) em matéria de proteção de dados.

> "Para melhorar os seus serviços, uma empresa privada substitui os pontos de controlo da identificação de passageiros no interior de um aeroporto (entrega de bagagem, embarque) por sistemas de videovigilância que utilizam técnicas de reconhecimento facial para verificar a identidade dos passageiros que optaram por consentir em tal procedimento. Uma vez que o tratamento se enquadra no artigo 9.º, os passageiros, que terão previamente dado o seu consentimento explícito e informado, terão de se inscrever num terminal automático, por exemplo, para criar e registar o seu modelo facial associado ao seu cartão de embarque e identidade. Os pontos de verificação com reconhecimento facial têm de ser claramente separados, por exemplo instalando o sistema dentro de um pórtico, para que os modelos biométricos das pessoas que não deram o seu consentimento não sejam captados. Apenas os passageiros que tenham dado previamente o seu consentimento e que tenham efetuado a inscrição utilizarão o pórtico equipado com o sistema biométrico."

Tendo-se chegado à conclusão de que os sistemas de monitorização da avaliação à distância que recorrem a técnicas de reconhecimento facial, implicam, de facto, um tratamento de categorias especiais de dados, importa agora aferir em que condições poderá esse mesmo tratamento ser lícito, sendo certo que terá de ocorrer uma das exceções previstas no n.º 2 do artigo 9.º do RGPD, para que se levante a proibição do seu tratamento. Aqui importa equacionar, em especial, a vontade do titular dos dados e o interesse prosseguido pelo responsável pelo tratamento (o interesse público e o interesse legítimo do responsável pelo tratamento, por regra em função da natureza pública ou privada do responsável).

4.1.1. Consentimento explícito do titular dos dados

A primeira possibilidade prevista no n.º 2 do artigo 9.º do RGPD, é o consentimento explícito do titular dos dados, salvo se o direito da União ou do Estado-Membro previr que a proibição em causa não possa ser levantada. Não será o caso, atenta a Lei n.º 58/2019, de 8 de agosto, e tendo em conta que o público alvo será maior de idade. Assim, o consentimento do aluno parece ser condição suficiente para o tratamento dos seus dados biométricos, desde que "livre, específico, informado e inequívoco", "mediante declaração ou ato positivo inequívoco", na aceção do disposto no ponto 11 do artigo 4.º do RGPD, e desde que se cumpram os princípios relativos ao tratamento de dados pessoais (artigo 5.º *ibid*.). No entanto, para que o consentimento seja efetivamente livre, sendo essa uma condição essencial para que se considere válido, de acordo com o ponto 3 das Diretrizes 05/2020 do CEPD [35]:

> "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. Ao solicitar o consentimento, os responsáveis pelo tratamento têm o dever de avaliar se irão cumprir todos os requisitos para obter um consentimento válido. Caso seja obtido em conformidade com o RGPD, o consentimento é um instrumento que permite aos titulares dos dados controlarem se os dados pessoais que lhes dizem respeito vão ou não ser tratados. Caso não o seja, o controlo do titular dos dados torna-se ilusório e o consentimento será um fundamento inválido para o tratamento, tornando essa atividade de tratamento ilícita[20]."

Assim, tendo em conta que o aluno se encontra numa posição de vulnerabilidade face ao estabelecimento no qual estuda (dado que a relação entre o estabelecimento de ensino e o estudante não é, de facto, paritária), poderá questionar-se se o seu consentimento é realmente livre. A este respeito, o considerando 42 do RGPD diz o seguinte:

> "Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.";

e ainda, o considerando 43, *ibid*.:

> "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. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução";

[20] Por reprodução da anotação à citação: Ver também o Parecer 15/2011 do Grupo de Trabalho do artigo 29.º sobre a definição de consentimento (WP 187), p. 6-8, e/ou o Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE (WP 217), p. 9, 10, 13 e 14.

por fim, prevê o n.º 4 do artigo 7.º, *ibid*., relativo às condições aplicáveis ao tratamento, que:

> "ao 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.".

Ainda de acordo com as Diretrizes 05/2020 do CEPD [35], no que se refere aos elementos do consentimento válido, diz o ponto 13:

> "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[21].".

A monitorização dos alunos, em contexto de avaliação à distância, baseada no consentimento livre (sem prejuízo do dever de ser também ele expresso, específico, informado e revogável) para o tratamento dos seus dados biométricos com recurso a técnicas de reconhecimento facial, implicaria sempre, que a eles fosse concedida a possibilidade de realizar a mesma avaliação sem se sujeitarem a tal forma de controlo. Assim, seria válida a alternativa de realização da mesma atividade em regime presencial, ou outra forma, desde que não implicasse o tratamento de dados biométricos, e quando praticada em iguais circunstâncias de dificuldade e tempo de duração, sem que optando por essa solução, resultassem consequência negativas para o aluno.

Este será, contudo, um método elegível para a licitude do tratamento de categorias especiais de dados.

4.1.2. 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 artigo 9.º do RGPD.

[21] Por reprodução da anotação à citação: Ver Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 12.

"*Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados*".

O tratamento de dados pessoais necessário à prestação do serviço público do ensino superior será, em princípio, legítimo se, de acordo com o estatuído pela alínea e) do n.º 1 do artigo 6.º, *ibid*.:

"*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*".

Contudo, no caso particular da categoria especiais de dados pessoais, o fundamento da alínea g) do n.º 2 do artigo 9.º do RGPD não requer só 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 acrescido que revela a necessidade de especial proteção dos dados tratados.

O tratamento de dados biométricos na aceção dos termos anteriores exigirá que esteja previsto pelo Direito da União Europeia ou nacional e de acordo com as demais disposições legais.

Da análise da Lei n.º 62/2007, de 10 de setembro, que aprova o regime jurídico das instituições de ensino superior, extrai-se o seguinte:

i. As instituições de ensino superior públicas são pessoas coletivas de direito público, podendo, porém, revestir também a forma de fundações públicas com regime de direito privado, estando sujeitas ao regime aplicável às demais pessoas coletivas de direito público de natureza administrativa (*cf.* n.º 1 e n.º 2 do artigo 9.º, *ibid*.);
ii. No caso particular das fundações, regem-se pelo direito privado, que não prejudica a aplicação dos princípios constitucionais respeitantes à Administração Pública, nomeadamente a prossecução do interesse público, bem como os princípios da igualdade, da imparcialidade, da justiça e da proporcionalidade (*cf.* n.º 1 e n.º 2 do artigo 134.º, *ibid*.).
iii. As instituições de ensino superior privadas regem-se pelo direito privado em tudo o que não for contrariado pela lei, *ibid*..

O DL n.º 74/2006, de 24 de março, que aprova o regime jurídico dos graus e diplomas do ensino superior, prevê no seu artigo 14.º, que o órgão legal e estatutariamente competente de cada

estabelecimento de ensino superior aprova normas, designadamente relativas ao regime de avaliação de conhecimentos.

Ora, ainda que em causa esteja uma instituição de ensino superior pública, na prossecução do interesse público, 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, uma vez que, pelo facto de este tratamento afetar dados pessoais especiais, portanto, sendo suscetível de impactar com maior risco nos direitos fundamentais dos alunos, tal dependerá sempre de se estatuir, sob a forma de lei, em que medida e circunstâncias a identificação dos estudantes, por via dos seus dados biométricos, poderia ser justificada como interesse público 'importante' (Considerando 52 do RGPD).

Este parece ser, no entanto, o caminho mais adequado quando em causa esteja a restrição de direitos fundamentais, mais especificamente, restrição de direitos, liberdades e garantias[22]. Aliás, o Considerando 52 do RGPD, prevê que a derrogação possa ser feita exatamente por motivos de ordem sanitária, incluindo de saúde pública. Ainda assim, a ser criado o referido diploma, haveria que o fazer em respeito pelos princípios da necessidade e proporcionalidade, sem esquecer as salvaguardas adequadas, submetendo-o ao parecer prévio da CNPD, no âmbito das suas atribuições e competências.

4.2. Tratamento para efeito dos interesses legítimos do responsável

A possibilidade de fundamentar o tratamento dos dados na sua necessidade para satisfação dos interesses legítimos prosseguidos pelo responsável pelo tratamento, salvo se prevalecerem os interesses ou direitos e liberdades fundamentais do titular dos dados, está prevista pela alínea f) do n.º 1 do artigo 6.º do RGPD.

Neste caso, não poderia nunca verificar-se um tratamento de dados que envolvesse reconhecimento facial, já que não estaria preenchido um qualquer apostolado, de entre os previstos, para o levantamento da proibição do tratamento de categorias especiais de dados pessoais (n.º 2 do artigo 9.º do RGPD).

Embora diferentes, os conceitos de «interesse» e de «finalidade» estão diretamente relacionados. A finalidade é a razão específica do tratamento dos dados, o objetivo ou a intenção. Um interesse é o objetivo mais abrangente que o responsável pelo tratamento pode ter, ou retirar do tratamento. Um interesse é legítimo quando for lícito (*i.e.,* quando o objetivo não for proibido pelo direito nacional e da UE); específico, *i.e.*, definido de forma clara para permitir uma ponderação face

[22] Cf. artigo 18.º e 165.º, n.º 1, alínea b), da Constituição da República Portuguesa.

aos interesses ou direitos e liberdades do titular dos dados; e representar um interesse real e atual [36]. De acordo com o considerando 47 do RGPD, temos:

por um lado, que

> "a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade",

por outro, que

> "o tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento."

A invocação do presente fundamento de licitude para tratamento dos dados, está expressamente subordinada a um teste da ponderação complementar, que exige que os interesses legítimos do responsável pelo tratamento sejam ponderados em relação aos interesses ou aos direitos fundamentais dos titulares em causa.

Por outro lado, o n.º 1 do artigo 21.º do RGPD, garante ao titular dos dados o direito de oposição ao tratamento[23], sendo particularmente especial ao assentar essencialmente na avaliação objetiva dos interesses e direitos envolvidos, permitindo que o titular em causa exerça a sua autodeterminação através de um direito de oposição - que não deve ser confundido com o consentimento baseado na alínea a) do n.º 1 do artigo 6.º, porque neste caso o tratamento não se pode realizar sem que o responsável obtenha o consentimento - salvo disposição legal em contrário. O titular dos dados, pode assim opor-se, em qualquer altura, por razões preponderantes e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objeto de tratamento. Acrescenta ainda o mesmo artigo que, em caso de oposição justificada, o tratamento deixa de poder incidir sobre esses dados. Em última análise, o responsável poderá ter que por termo àquele específico tratamento [36].

Em suma, um tratamento de dados que se baseie no fundamento de licitude aqui analisado, sempre dependerá de estarem reunidas as seguintes condições: não prevalecerem os interesses ou direitos e liberdades fundamentais do titular dos dados; uma avaliação cuidada da qual se conclua ser expectável para o titular, no momento em que facultou os seus dados, que os mesmos seriam usados para esta esta finalidade; e que o titular possa, em termos práticos e a todo o tempo, acionar o direito

[23] Sempre que o tratamento dos dados seja baseado nas alíneas e) e f) do n.º 1, do artigo 6º do RGPD, ou no n.º 4 do mesmo artigo e diploma.

de oposição ao tratamento de dados em causa (direito legalmente concedido, através do artigo 21.º do RGPD).

4.3. Transferências internacionais de dados: em especial, os EUA

Considerando agora as condições de licitude que o RGPD, no seu capítulo V, impõe especificamente para a transferência de dados pessoais para países terceiros, recorda-se que o acórdão do Tribunal de Justiça da União Europeia (TJUE), de 16 de julho de 2020, celebremente conhecido como acórdão 'Schrems II'[24], concluiu que as transferências de dados pessoais da UE para os EUA não asseguram um nível de proteção adequado, ou seja, equivalente ao que é assegurado na UE.

A legislação nacional dos EUA, em particular, no âmbito dos programas de vigilância baseados na secção 702 da FISA, tais como o PRISM[25] e o UPSTREAM[26], coloca à disposição das Autoridades norte-americanas o acesso a dados pessoais para fins de segurança nacional. Por outro lado, a legislação norte-americana não concede aos titulares dos dados europeus, direitos acionáveis perante os tribunais contra as Autoridades dos EUA (cf. ponto 192 do acórdão) [37].

Assim, deduziu o TJUE que as transferências de dados pessoais da UE para os EUA são contrárias ao RGPD e à Carta dos Direitos Fundamentais da UE, a menos que sejam acrescentadas salvaguardas adicionais ou as transferências sejam justificadas ao abrigo do artigo 49.º do RGPD (que permite derrogações em situações específicas[27]) [39].

Por conseguinte, as organizações públicas e privadas ficaram obrigadas à adoção de medidas complementares, devendo privilegiar soluções que cumpram o RGPD, nomeadamente quando utilizam soluções de computação na nuvem (*cloud computing*), de empresas sediadas nos EUA, já que as mesmas estão sujeitas à lei norte-americana (o mesmo valendo para as transferências para os demais Estados terceiros que não assegurem um nível adequado de proteção). As Autoridades de proteção de dados estão obrigadas a suspender ou a proibir a transferências de dados, mesmo quando assentes em contratos baseados no modelo aprovado pela Comissão Europeia, se não houver garantias de que aquelas medidas são respeitadas no país terceiro [40].

No caso particular das aplicações de monitorização de alunos é especialmente grave a transferência de dados pessoais nas condições anteriores, sobretudo quando estejam envolvidas

[24] A propósito da queixa na sua origem, apresentada por Maximillian Schrems (fundador da NOYB – *European Center for Digital Rights*), enquanto utilizador do Facebook, relativa à transferência dos seus dados pessoais pela Facebook Ireland para a Facebook Inc., nos Estados Unidos.
[25] Compilação de comunicações provenientes de empresas como Google, Yahoo e Facebook (Meta) [30].
[26] Interseção de comunicações ao nível do *backbone* [36].
[27] A este propósito, foram disponibilizadas pelo EDPB as Recomendações 01/2020, relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE [38].

categorias especiais de dados pessoais, por permitirem identificar o seu titular de forma inequívoca. Pela mesma razão se compreenderá revestir-se de especial gravidade, sempre que ocorra essa transferência de dados baseada num qualquer outro fundamento de licitude que não o consentimento do titular dos dados, por este não ter qualquer intervenção no processo de decisão.

4.4. A IA e o direito ao apagamento

Relevante é ainda analisar em que medida o contexto da monitorização da avaliação, com recurso a técnicas de reconhecimento facial, assegura os direitos dos titulares dos dados, máxime, o direito ao apagamento dos dados pessoais. O artigo 17.º do RGPD prevê que o titular dos dados tenha o direito de solicitar, ao responsável pelo tratamento, o apagamento dos dados pessoais que lhe digam respeito. Por sua vez, o segundo tem a obrigação de apagar os dados pessoais, sem demora injustificada, nas situações previstas naquele artigo, designadamente quando os dados deixam de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

Sem prejuízo da discussão que se poderá originar em torno da definição desse momento, certo será que, algures no tempo, os dados deixarão muito provavelmente de ser necessários para a finalidade que motivou a sua recolha ou tratamento.

Ora, o exercício do direito ao apagamento pelo titular dos dados, revestir-se-á de caráter peculiar quando em causa estejam sistemas de aprendizagem automática (*machine learning)*, não apenas pela sua complexidade natural, mas também por se tratarem de sistemas concebidos essencialmente para a otimização dos resultados gerados. Para tanto, contribui a quantidade de informação fornecida – dados de aprendizagem (*datasets*) – tratada pelo respetivo algoritmo, encarregue de construir um conjunto de regras que darão origem ao modelo de dados de resposta. Por essa mesma razão, não lhe são conhecidas especiais funcionalidades relativas à eliminação dos dados. A informação é a peça chave. Se dela se não dispuser de todo, ou em quantidade suficiente, os resultados refletirão essa consequência.

Ao facultarmos a um algoritmo tantos vídeos quantos os necessários, para que este aprenda a detetar, num determinado momento, quando uma pessoa se encontra a falar, o algoritmo irá criar um extenso conjunto de regras baseadas na informação facultada e que no final lhe permitirá aferir, com maior ou menor precisão, se num dado novo vídeo alguém se encontra a falar. Este largo conjunto de regras criadas pelo algoritmo, só por si, não constitui informação pessoal, já que não deverá ser passível de ser revertida e assim permitir chegar-se aos dados que lhe deram origem [41], [42].

No entanto, o mesmo não se verifica durante o processo de agregação dos dados para aprendizagem e da sua disponibilização ao algoritmo. Tendo em conta ser constantemente necessário proceder a ajustes, tanto na correção como no aumento de específicos dados de amostragem, ou ainda de melhorias algorítmicas, será de esperar não só que se guardem os dados de aprendizagem já adquiridos, como também, se possível, aqueles que venham a ser alvo de tratamento pelo modelo.

Embora não seja determinístico o impacto num novo modelo de dados, quando se remove uma amostra, ou um subconjunto de amostras pouco expressivas face ao modelo anterior, certo será que se for apagado um subconjunto de amostras significativamente representativas de uma

determinada característica, as consequências irão repercutir-se, podendo compreender a introdução de entropia na eficácia do algoritmo ou, porventura, na sua efetiva capacidade de resposta [42].

A título de exemplo, tome-se um conjunto de titulares de dados possuidores de uma determinada característica facial rara, comum entre si, e que autorizam o tratamento de fotografias suas para permitir ao algoritmo distingui-los dos demais. Se, num determinado dia, esse conjunto de pessoas solicitar o apagamento das suas fotografias, que serviram para a aprendizagem do algoritmo, as compilações de modelos posteriores ao seu apagamento resultarão na incapacidade de resposta adequada, quando o novo modelo for confrontado com uma fotografia de alguém com semelhantes características, podendo conduzir a uma situação de discriminação.

Naturalmente existirão desafios, porventura sem uma resposta óbvia. No entanto, será possível conjugar a AI e as garantias da proteção dos dados previstas pelo RGPD, desde que as mesmas sejam consideradas desde a fase do desenvolvimento, à da utilização do modelo. Para tanto, os algoritmos deverão ser construídos de forma a que sejam robustos à eventual retificação ou eliminação de parte dos dados de aprendizagem. Deverão ainda ser construídos com base nos princípios da proteção dos dados desde a conceção e por defeito. Aumentar a quantidade dos dados de aprendizagem e variar a origem desses dados, contribuirá para criar resiliência ao apagamento de alguns deles. Na recolha de dados de aprendizagem, ainda que a celebração de contratos possa representar um custo adicional, será à partida o meio que garante maior duração dos dados recolhidos. Deverá adotar-se o princípio da minimização dos dados, sempre que possível através da sua anonimização, ou na sua impossibilidade, tratar apenas os dados estritamente necessários. Adotar medidas necessárias à prevenção de ataques que comprometam integridade do sistema de IA (*e.g.* ML *poisoning attacks* [43], [44]) [42].

Deverá também ter-se em linha de consideração o artigo 16º do RGPD que garante ao titular dos dados o direito de obter do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Este cenário terá igualmente de ser acomodado, sobretudo quando em causa estejam algoritmos de decisão baseados no perfil da pessoa (*profiling)*, que poderá conduzir a situações de 'falsos positivos'. A situação tornar-se-á ainda mais grave se esses dados forem posteriormente adicionados ao conjunto de dados de aprendizagem (*e.g.* deteção de comportamentos fraudulentos ou suscetíveis de constituírem fraude).

CAPÍTULO 5

Conclusões

O processo de avaliação de conhecimentos à distância admite, sobretudo, discricionariedade física e geográfica do local de realização da prova. Por conferir equidade de acesso, permite que alunos com limitações físicas ou de saúde, oriundos, ou que por força das circunstâncias se encontrem em localização distante à do estabelecimento de ensino, realizem a prova de conhecimentos sem esforço ou custos acrescidos. Se o processo de avaliação for totalmente digital, poderá ainda permitir corrigir, de forma automática, os exercícios que não sejam de resposta aberta (*e.g.* escolha múltipla, exercícios de correspondência), reduzindo tanto o tempo de correção como o erro intrinsecamente associado.

No entanto, para que seja igualmente equitativo face aos demais, importará conferir-lhe idênticos mecanismos de prevenção de fraude.

Este estudo confirmou serem várias as soluções de mercado que se propõem a esse fim, sendo igualmente diversos os métodos e tecnologias a que recorrem, implicando um maior ou menor risco associado ao tratamento dos dados pessoais. Por esse motivo, as instituições que pretendam incluir o regime de avaliação à distância, adotando mecanismos de monitorização, deverão ponderar a sua efetiva necessidade, condições de aplicabilidade, os riscos associados às ferramentas ou sistemas que pretendam usar, bem como as condições de licitude da sua utilização. De forma geral, mas não exaustiva, deverão observar o seguinte:

- Reconhecimento desse regime de avaliação, pelo órgão legal e estatutariamente competente da respetiva instituição de ensino superior (DL n.º 74/2006, de 24 de março), permitindo apreciar as reais necessidades, caso a caso, definindo as circunstâncias específicas ou critérios ponderosos que justifiquem o uso dos meios que venham a ser propostos.
- No ponto 3.1 do Capítulo terceiro, foi apresentada uma proposta de categorização das soluções de monitorização, compreendendo a monitorização em tempo real, recurso à gravação de vídeo, e monitorização automática, admitindo-se, no entanto, a sua conjugação. Qualquer que seja a solução ambicionada, além da imprescindibilidade de cumprir as disposições legais em matéria de proteção de dados, deverá permitir alcançar os mesmos fins (eficácia na deteção de fraude), revelando-se menos restritiva dos direitos dos titulares e dos princípios relativos ao tratamento de dados pessoais.
- Para tanto, admitindo-se o recurso ao tratamento de dados biométricos enquanto categoria especial de dados pessoais do RGPD, lembrando que ali caberá a definição de identificação

biométrica (comparação de 'um para muitos'), o fundamento da licitude deverá basear-se no consentimento do titular dos dados.

- O consentimento do titular, ao ter que ser livre, expresso, específico, informado e revogável, implicará sempre que o aluno possa realizar a mesma avaliação, em iguais circunstâncias de dificuldade, por outro meio que não envolva o tratamento dos dados – aqui se entenderá, por via da avaliação em regime presencial.
- Se, por outro lado, o tratamento dos dados, incluindo de categorias especiais de dados, se basear no interesse público, sempre terá o legislador que regular a medida e circunstâncias em que tal possa acontecer, salvaguardando o respeito pelos princípios da necessidade e da proporcionalidade.
- Ressalva-se, ainda, que se o tratamento de dados for justificado para efeito dos interesses legítimos do responsável (leia-se, estabelecimento de ensino superior), sempre terá de se verificar se não prevalecem os interesses ou direitos e liberdades dos titulares dos dados (examinandos), que, a verificar-se, impedirá o tratamento dos dados. Mesmo que superando este exercício de ponderação, terá sempre que se assegurar ao titular dos dados o respetivo direito de oposição ao tratamento.
- Se o tratamento de dados apenas se basear no fundamento de licitude anterior, não poderá ocorrer o tratamento de categorias especiais de dados, de onde se engloba a identificação biométrica, por se não verificar qualquer uma das exceções para o levantamento da sua proibição.
- A utilização de mecanismos de reconhecimento facial que utilizem dados biométricos, requer não só a necessária base legal, como também uma análise documentada dos riscos associados ao tratamento dos dados, da qual deverá decorrer a adoção de garantias específicas, sem esquecer, no caso de contratação de tais serviços a terceiros, a necessária e prévia autorização, por escrito, do responsável pelo tratamento (artigo 28.º do RGPD).
- O tratamento de dados pessoais que implique a sua transferência para países terceiros sem proteção adequada requer a adoção de medidas suplementares que permitam assegurar um nível de proteção essencialmente equivalente ao garantido na União Europeia.
- Os algoritmos de IA devem ser estruturalmente resilientes e construídos com base nos princípios da proteção dos dados desde a conceção e por defeito, por forma a acautelar a garantia dos direitos de retificação e de apagamento dos dados, respetivamente, artigos 16.º e 17.º do RGPD.
- Deverão ainda observar o princípio da minimização dos dados, sempre que possível, de forma anonimizada.

Referências legislativas

Decreto-Lei n.º 10-A/2020, de 13 de março, estabelece medidas excecionais e temporárias relativas à situação epidemiológica do novo Coronavírus - COVID 19.

Decreto-Lei n.º 20-H/2020, de 14 de maio, estabelece medidas excecionais de organização e funcionamento das atividades educativas e formativas, no âmbito da pandemia da doença COVID-19.

Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados - revogada.

Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) – e consequentes retificações de 23 de maio de 2018 e de 4 de março de 2021.

Acórdão proferido pelo Tribunal de Justiça da União Europeia, de 16 de julho de 2020, no âmbito do processo C-311/18.

Carta dos Direitos Fundamentais da União Europeia

Foreign Intelligence Surveillance Act Of 1978 Amendments Act Of 2008

Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas)

Decreto-Lei n.º 74/2006, de 24 de março, aprova o regime jurídico dos graus e diplomas do ensino superior, em desenvolvimento do disposto nos artigos 13.º a 15.º da Lei n.º 46/86, de 14 de Outubro (Lei de Bases do Sistema Educativo), bem como o disposto no n.º 4 do artigo 16.º da Lei n.º 37/2003, de 22 de Agosto (estabelece as bases do financiamento do ensino superior).

Constituição da República Portuguesa

Referências bibliográficas

[1] D. Fletcher (2015, jun.). Pearson VUE expands exam delivery with ProctorCam acquisition [Em linha]. Disponível em: https://home.pearsonvue.com/About-Pearson-VUE/Press-Room/2015/Pearson-VUE-expands-exam-delivery-with-ProctorCam.aspx [2022, 23 nov.]

[2] P. Pascale (2019, mar.). Pearson VUE introduces next generation of online proctoring solution, OnVUE [Em linha]. Disponível em: https://home.pearsonvue.com/About-Pearson-VUE/Press-Room/2019/Pearson-VUE-introduces-next-generation-of-online-p.aspx [2022, 23 nov.]

[3] T. Reed (2020, fev.). McGraw-Hill Selects Proctorio to Deliver Remote Proctoring and Browser Locking Capabilities Within its Digital Course Materials. [Em linha]. Disponível em: https://www.mheducation.com/news-media/press-releases/mcgraw-hill-proctorio-delivers-remote-proctoring.html [2022, 23 nov.]

[4] Gabinete do Ministro Da Ciência, Tecnologia e Ensino Superior (2020, abr.). Recomendação às instituições científicas e de ensino superior relativamente à cessação do estado de emergência motivado pela pandemia COVID-19. [Em linha]. Disponível em: https://wwwcdn.dges.gov.pt/sites/default/files/comunicado_mctes_fim_de_estado_de_emergencia_v30abril2020.pdf [2022, 23 nov.]

[5] Gabinete do Ministro Da Ciência, Tecnologia e Ensino Superior (2020, maio). Recomendação às instituições científicas e de ensino superior para garantir o processo de reativação faseada e responsável das atividades na presença de estudantes, docentes e investigadores. [Em linha]. Disponível em: https://wwwcdn.dges.gov.pt/sites/default/files/comunicado_mctes_desconfinamento_v15maio2020_rev_1.pdf [2022, 23 nov.]

[6] Comissão Nacional de Proteção de Dados (2020, maio). Orientações sobre avaliação à distância nos estabelecimentos de ensino superior. [Em linha]. Disponível em: https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf [2022, 23 nov.]

[7] Comissão Nacional de Proteção de Dados (2020, abril). Orientações para utilização de tecnologias de suporte ao ensino à distância. [Em linha]. Disponível em: https://www.cnpd.pt/media/0mwfxdcp/orientacoes_avaliacao_distancia_ensino_superior.pdf [2022, 23 nov.]

[8] FCCN. "Piloto de Sistemas de Avaliação Remota." [Em linha]. Disponível em: https://www.fccn.pt/inovacao/piloto-sistemas-avaliacao-remota (Assessed Nov. 15, 2020).

[9] Metared (2020, 22 abril). Webinar: "Ferramentas de Avaliação remota. Dúvidas e soluções" [Em linha]. Disponível em: https://eventos.metared.org/51621/detail/ferramentas-de-avaliacao-remota-duvidas-e-solucoes.html [2022, 23 Nov.]

[10] R. Ribeiro, P. Cabral, and J. Gomes, “Relatório final: Sistemas de Avaliação Remota” FCT and FCCN, Lisbon, Portugal, Rep. EXT/2020/1/ASA.NAU, 2020

[11] Comissão Nacional de Proteção de Dados (2021, maio). Deliberação/2021/622. [Em linha]. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121887 [2022, 23 nov.]

[12] Garante per la Protezione dei Dati Personali. “Ordinanza ingiunzione nei confronti di Università Commerciale “Luigi Bocconi” di Milano - 16 settembre 2021.” [Em linha]. Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9703988 [2022, 23 Nov.].

[13] Datatilsynet. “Universitets brug af tilsynsprogram ved online eksamen” [Em linha] Disponível em: https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/jan/universitets-brug-af-tilsynsprogram-ved-online-eksamen [2022, 23 Nov.].

[14] Hoge Raad der Nederlanden en Raad van State. “ECLI: NL: RBAMS: 2020: 2917” [Em linha] Disponível em: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917 [2022, 23 Nov.].

[15] Comissão Nacional de Proteção de Dados (2019, set.). Deliberação/2019/494. [Em linha]. Disponível em: https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/121704 [2022, 29 nov.]

[19] F. P. Coutinho “A Independência da Comissão Nacional de Proteção de Dados,” *Anuário da Proteção de Dados, (2020), pp. 9 – 47*.

[17] Jornal Oficial da União Europeia, “Retificação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho,” 4 março 2021. [Em linha]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2021.074.01.0035.01.POR&toc=OJ:L:2021:074:TOC. [2022, 23 Nov.].

[18] F. R. Rocha, Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019, março 2021, pp. 238-244, ISBN 978-972-40-9261-4.

[19] L. Jasmontaine, I. Kamara, G. Zanfir-Fortuna, S. Leucci. “Data Protection by Design and by Default: Framing Guiding Principles into Legal Obligations in the GDPR,” *European Data Protection Law Review, Volume 4, Issue 2 (2018), pp. 168 – 189*, doi: 10.21552/edpl/2018/2/7.

[20] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices” (maio, 2010; revised: jan. 2011). [Em linha] Disponível em: Information and Privacy Commissioner of Ontario, Disponível em: https://www.ipc.on.ca. [2022, 23 Nov.].

[21] OECD, “OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, Organisation for Economic Co-operation and Development (OECD), 2013. (pp. 23-25) [Em linha]. Disponível em: https://www.oas.org/es/sla/ddi/docs/OECD%20Guidelines%20Governing%20the%20Protection%20on%20Privacy%20and%20Transborder%20Flows%20of%20Personal%20Data.pdf. [2022, 23 Nov.].

[22] OECD, “The OECD Privacy Framework: Evolution and innovation in privacy governance”, Organisation for Economic Co-operation and Development (OECD), 2013, (pp. 68, 69, 103-105) [Em linha]. Disponível em: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [2022, 23 Nov.].

[23] Resolution on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 out. 2010, Jerusalém, Israel [Em linha]. Disponível

emhttps://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf. [2022, 23 Nov.].

[24] Comité Europeu para a Proteção de Dados, “Orientações 4/2019 relativas ao artigo 25.º Proteção de Dados desde a Conceção e por Defeito”. (p. 14) [Em linha]. Disponível em: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_pt.pdf. [2022, 23 Nov.].

[25] Article 29 Data Protection Working Party (WP29), “Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones”. [Em linha]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf. [2022, 23 Nov.].

[26] European Union Agency for Cybersecurity, “Privacy and Data Protection by Design,” 2015. [Em linha]. Disponível em: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design. [2022, 23 Nov.].

[27] World Wide Web Consortium (W3C), “Tracking Preference Expression (DNT),” 2019. [Em linha]. Disponível em: https://www.w3.org/TR/tracking-dnt. [2022, 23 Nov.].

[28] A. ElBanna and N. Abdelbaki, "Browsers Fingerprinting Motives, Methods, and Countermeasures," *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 2018, pp. 1-5, doi: 10.1109/CITS.2018.8440163.

[29] K. V. Nair and E. RoseLalson, "The Unique Id's you Can't Delete: Browser Fingerprints," *2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR)*, 2018, pp. 1-5, doi: 10.1109/ICETIETR.2018.8529040.

[30] G. O’Reilly, J. Creagh, “A categorization of Online Proctoring”, in *Proceedings of Global Learn-Global Conference on Learning and Technology*, 2016, pp. 542-552.

[31] S. Arnò, A. Galassi, M. Tommasi, A. Saggino, P. Vittorini, “State-of-the-Art of Commercial Proctoring Systems and Their Use in Academic Online Exams”, 2021 International Journal of Distance Education Technologies, Volume 19, Issue 2, April-June 2021, doi: 10.4018/IJDET.20210401.oa3

[32] Article 29 Data Protection Working Party (WP29), “Opinion 3/2012 on developments in biometric technologies”. [Em linha]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. [2022, 23 Nov.].

[33] Comissão Europeia, “Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança”. [Em linha]. Disponível em: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf. [2022, 23 Nov.].

[34] Comissão Europeia, “Diretriz 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo.”, 29 jan. 2020, v. 2.0 [Em linha]. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf. [2022, 23 Nov.].

[35] Comissão Europeia, “Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679”, 4 maio 2020, v. 1.1 [Em linha]. Disponível em:

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. [2022, 23 Nov.].

[36] Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, "Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE", 9 abril 2014, [Em linha]. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf. [2022, 23 Nov.].

[37] Electronic Frontier Foundation (EFF), "Upstream vs. PRISM". [Em linha]. Disponível em: https://www.eff.org/pages/upstream-prism. [2022, 23 Nov.].

[38] CNIL, "CNIL calls for changes in the use of US collaborative tools by French universities", 31 maio 2021 [Em linha]. Disponível em: https://www.cnil.fr/en/cnil-calls-changes-use-us-collaborative-tools-french-universities [2022, 23 Nov.].

[39] European Data Protection Board (EDPB), "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data". [Em linha]. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf. [2022, 23 Nov.].

[40] InfoCuria, "Acórdão Do Tribunal De Justiça no processo C-311/18)", 16 julho 2020 [Em linha]. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=1ADE24410C55C93DBB45CC1ABEA27F2A?text=&docid=228677&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=6050727 [2022, 23 Nov.].

[41] CNPD, "Censos 2021: CNPD suspende fluxos para os EUA", 27 abril 2021 [Em linha]. Disponível em: https://www.cnpd.pt/comunicacao-publica/noticias/censos-2021-cnpd-suspende-fluxos-para-os-eua/ [2022, 23 Nov.].

[42] Datatilsynet "Artificial intelligence and privacy," January, 2018, [Em linha]. Disponível em: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [2022, 23 Nov.].

[43] T. S. Cabral. "Forgetful AI: AI and the Right to Erasure under the GDPR," *European Data Protection Law Review, Volume 6, Issue 3 (2020)*, pp. 378–389, doi: 10.21552/edpl/2020/3/8.

[44] A. Oprea, A. Singhal, A. Vassilev, "Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy?" em Computer, vol. 55, no. 11, pp. 94-99, 2022. doi: 10.1109/MC.2022.3190787

[45] E. Tabassi, K. Burns, M. Hadjimichael, A. Molina-Markham, e J. Sexton, "A taxonomy and terminology of adversarial machine learning,", 30 out. 2019 [Em linha]. Available: https://csrc.nist.gov/publications/detail/nistir/8269/draft [2022, 23 Nov.].

ANEXO A

Artigo para publicação no Anuário da Proteção de Dados do Observatório para a Proteção de Dados Pessoais

Avaliação de conhecimentos à distância no ensino superior português: processos de monitorização e sua conformidade com o RGPD

Saul A. N. Ferreira Leite[*]

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 à distância, que algumas acabariam por adotar.

O presente estudo propõe-se a seguir uma proposta de classificação dessas soluções identificando, em cada caso, as 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 à 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 this means to continue 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, in each 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.

Declaração de princípio

A presente reflexão resulta da visão pessoal do seu autor e do trabalho desenvolvido em sede académica, não vinculando a posição da instituição na qual desempenha funções.

[*] Licenciado em Engenharia de Telecomunicações e Informática pelo Iscte – Instituto Universitário de Lisboa.

1. Introdução

As aplicações informáticas que se propõem à monitorização de um processo de avaliação de conhecimentos à 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[2], 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[3]. As restrições acabariam ainda por se fazer sentir com a declaração do estado de calamidade[4], que vigorou entre 1 e 30 de maio de 2021.

O direito ao ensino - constitucionalmente previsto[5] *(mens legis)* - levou a que as instituições de ensino superior optassem pelos meios mais adequados à continuidade das atividades letivas, necessariamente à distância, equacionando, por outro lado, alternativas ao tradicional regime de avaliação.

A colocação em prática de um regime de avaliação à distância sempre suscitaria questões de âmbito legal e relativas à sua eficácia, ou ainda, relativamente ao processo de monitorização dos alunos, uma cuidada ponderação sobre o risco de ingerência nos seus direitos e liberdades fundamentais.

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 à distância – Piloto SAR[6] – para avaliar a experiência de utilização em ambiente de testes (provas de avaliação fictícias), de quatro soluções comerciais de monitorização à distância[7]. O projeto terminaria em julho do mesmo ano, concluindo[8] que as soluções comerciais em geral, e particularmente

---

[2] 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.

[3] 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*>.

[4] 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.

[5] Art.º 74.º, da Constituição da República Portuguesa.

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

[7] 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.

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

as 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*[9] realizado a 22 de maio de 2020, organizado em parceria pela *MetaRed Portugal*[10] 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 adequada análise dos respetivos tratamentos de dados à luz do Regulamento Geral sobre a Proteção de Dados (RGPD).

Se o é 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, sobretudo caracterizado pelo ensino simultaneamente em regime presencial[11] e à distância, algumas universidades portuguesas determinaram[12] a adoção de um regime avaliação de conhecimentos à distância, em alguns casos obrigatório.

Não tardaria, contudo, à semelhança do que aconteceu noutros países[13], que os visados se insurgissem[14] contra a realização das provas sob determinadas condições, ou pela utilização de determinados *softwares,* por entenderem estar em causa a violação do RGPD, da Lei n.º 58/2019, de 8 de agosto e das orientações da Comissão Nacional e proteção de Dados (CNPD)[15].

---

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

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

[11] 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.

[12] Por via da publicação do Despacho Reitoral nº 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 à 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.

[13] 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.

[14] (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*>.

[15] 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*>)

Nesta senda, viria a CNPD deliberar[16] 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, proporcionalidade e da minimização dos dados - todos do RGPD - e 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. 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.

Um pouco por toda a Europa verificaram-se episódios semelhantes, embora com desfechos variados. Em setembro de 2021, a 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, durante a utilização de um sistema para monitorização dos alunos. Na mesma deliberação[17] 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 dos riscos e a violação do princípio geral das transferências (artigo 44.º, em consonância com os Considerandos 101 e 102, do RGPD).

Num outro caso[18], 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), após a mesma se ter socorrido da utilização do *software ProctorExam,* para monitorizar os alunos no processo de avaliação à distância de uma disciplina[19]. 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)

---

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

[17] "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*>.

[18] "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*>

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

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.

Atendendo à retrospetiva traçada, o presente estudo propõe-se a seguir um modelo para a categorização das soluções de avaliação à distância, por forma a melhor enquadrar as respetivas características e funcionalidades. 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.

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[20], 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 à 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, legalmente capacitadas para optar por um regime de avaliação de conhecimentos à 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, pela Agência de Avaliação e Acreditação do Ensino Superior (A3ES)[21].

3. Soluções de monitorização: categorias e funcionalidades

As ferramentas que se propõem à monitorização da avaliação à distância fazem uso dos recursos do dispositivo do avaliado, entre os quais se incluem a *webcam*, o microfone e a ligação à internet, podendo

[20] 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.
[21] Criada pelo Decreto-Lei n.º 369/2007, de 5 de novembro.

ser essencialmente enquadradas nas seguintes categorias[22], sem prejuízo da possibilidade de 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[23] 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);
- 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 a 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 outro que seja construído a partir de uma fotografia captada no momento. De igual modo,

[22] 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.
[23] 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

embora sem casos conhecidos, será possível aplicar o mesmo princípio para o reconhecimento da voz do aluno, da sua impressão digital, íris, ou outros seus dados biométricos.

- Compatibilidade com dispositivos móveis iOS e/ou Android[24], enquanto meios complementares à monitorização do aluno e do espaço físico em 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).
- Gravação e/ou transmissão em tempo real de áudio e vídeo do examinando. Possibilidade, consoante as aplicações, de sinalização de comportamentos suspeitos e 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 360º com sua *webcam,* gravando um vídeo do local e das condições em que o exame foi 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, se a solução considerar que o aluno adotou um comportamento classificado fraudulento.
- Comunicação em tempo real (*live chat*), entre vigilante e examinando.

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

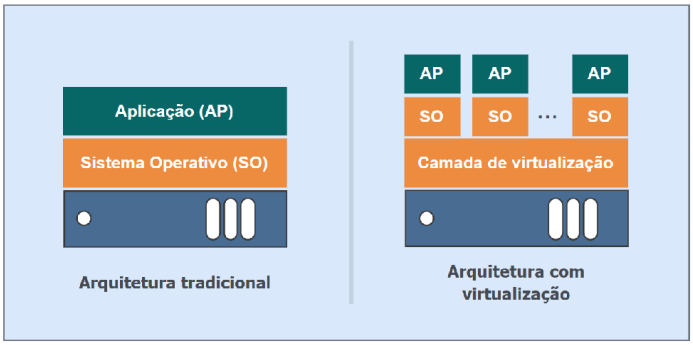

Figura 1 - Arquitetura tradicional e com virtualização.

A maioria das soluções de monitorização requer a instalação de uma aplicação no dispositivo do aluno (geralmente compatível com SO Microsoft Windows) e/ou de um *plugin* para o navegador *web*.

É possível combinar a monitorização em tempo real com a monitorização automática, verificando-se, numa base continua, 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 pode ter seu dispor um canal de comunicação (*live chat*) para alertar o aluno sobre as condutas inapropriadas.

De um modo geral, as soluções de monitorização recorrem a serviços prestados por terceiros, designadamente para alojamento da informação, processamento, reconhecimento de voz ou transcrição de discursos[25].

As soluções que oferecem monitorização automática recorrem sobretudo à computação em nuvem (*cloud computing*), para satisfazer os elevados recursos computacionais exigidos pela tecnologia de IA. Por outro lado, centram em si a complexidade associada à gestão e manutenção da infraestrutura de suporte à solução, disponibilizando a sua utilização numa lógica de *software-as-a-service* (SaaS).

3.1 Exemplos de ferramentas e respetivas particularidades

Para melhor evidenciar as funcionalidades presentes em cada categoria de monitorização, analisaram-se sete ferramentas comerciais: *ExamNet, ProctorExam e Respondus,* - testadas no Piloto

[25] Disponível em: *https://aws.amazon.com/blogs/publicsector/how-cloud-can-help-educational-institutions-grading-assessments-admissions*

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 foi recolhida entre janeiro e fevereiro de 2023, nos respetivos sítios *web* e nos fóruns e *blogs* oficiais. Assinala-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 é praticamente inexistente ou encontra-se se forma muito dispersa e, ainda assim, insuficiente.

- *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 aceder ao sítio[27] do projeto, através de um navegador *web*.

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 (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*

[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*>
[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]

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 um serviço da FCT/FCCN[31] que funciona sobre a aplicação de videoconferência - norte americana - Zoom[32], permitindo a sua integração com a plataforma de ensino *Moodle,* tendo sido disponibilizado para permitir a realização de aulas e reuniões à distância. Após a conclusão do Piloto SAR foi também adotado, 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 aplicabilidade na monitorização da avaliação à distância apresenta determinadas limitações, mas também vantagens face às congéneres. 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 de dispositivos móveis, que podem ser utilizados de forma complementar. De acordo com o sítio oficial[36] e com o Manual de Utilizador[37], o Colibri permite a gravação das sessões em *cloud,* sem que se especifique qual, embora, ao que tudo indica, determinada pela *Zoom*

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

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 venha a adicionar, modificar ou remover.

- *Safe Exam Browser (SEB)*

É um navegador *web* com características particulares, permitindo 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.

Atualmente, o SEB permite também a integração (opcional) com as aplicações *Jitsi* e *Zoom*, conferindo-lhe 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*

---

[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.

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

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 capturadas em provas anteriores, e que estão disponíveis durante o período de tempo definido 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 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].

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

- *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 à distância com monitorização automática, através das componentes *LockDown Browser* e *Monitor.* A primeira confere as capacidades anteriormente descritas, enquanto que a segunda guia o 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 à 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 à 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 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 ao direito de alterar a lista de subcontratantes, em

[45] Cf. disponível em: *https://web.respondus.com/wp-content/uploads/2021/03/RespondusMonitor_Scenarios.pdf*
[46] Motivo, pelo qual, se considera suportar a monitorização com recurso à gravação de vídeo.
[47] Cf. 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>.*

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 armazenamento), cabendo ao responsável pelo tratamento a tarefa de recolher, junto dos titulares, o respetivo consentimento. O ponto 2.4, relativo às medidas 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.

- ProctorExam

É uma das soluções que, desde a realização do Piloto SAR até à atualidade, alterou de uma infraestrutura gerida pelo responsável pelo tratamento, para o modelo de SaaS, 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*[50] específico para o navegador *Google Chrome*.

Segundo o sítio *web* da solução[51], 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 e do endereço IP[52] do examinando, como que não constituindo, também ela, dados pessoais.

A solução *ProctorExam* assume-se de harmonia com o RGPD. No entanto, não deixa de ser curioso que uma mera visita ao seu sítio *web* seja condição suficiente para um atropelo da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa à privacidade e às comunicações eletrónicas, mormente pela instalação de testemunhos de conexão (*cookies*) que não são estritamente

[49] Disponível em: <*https://web.respondus.com/privacy/subprocessors*>.
[50] Disponível em: <*https://chrome.google.com/webstore/detail/proctorexam-screen-sharin/digojkgonhgmnohbapdfjllpnmjmdhpg*>.
[51] Informação disponível em: <*https://proctorexam.com/privacy-and-data-security*>, [12 jan. 2023].
[52] 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.

necessários àquele propósito e que permitem a identificação do utilizador. Por conseguinte, não respeita os pressupostos legais relativos ao consentimento, previstos no RGPD.

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 *plugin 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 - Relação das características e funcionalidades das soluções de monitorização descritas, em função da sua categoria.

As soluções de monitorização são tão atraentes, quanto melhor se revele a sua eficácia na prevenção e deteção de fraude académica. A informação que disponibilizam acerca dos dados tratados é geralmente insuficiente, para que o responsável pelo tratamento possa decidir pela sua opção, de forma

consciente. No entanto, é ao último que cabe assegurar-se de que o tratamento dos dados é realizado em conformidade com o RGPD (cf. art.º 24.º do mesmo diploma).

4. Fundamentos de licitude para o tratamento de dados pessoais

No que respeita aos fundamentos jurídicos para o tratamento de dados prosseguido 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 fundamentar o tratamento de dados associado aos modelos de monitorização em tempo real e com recurso à gravação de vídeo, perfilam-se como candidatos naturais, as alíneas a), e) ou f) do n.º 1, art.º 6.º do RGPD.

Refira-se, porém, que o segundo parágrafo[53] do n.º 1, *ibid.*, veda às autoridades públicas na prossecução das suas atribuições a possibilidade de evocação da alínea f), na medida em que os interesses prosseguidos pelas mesmas podem apenas corresponder a interesses públicos, e nessa medida, determinados por lei[54].

4.1.1 Consentimento explícito do titular dos dados

Remetendo-nos à alínea a) do n.º 1, do art.º 6.º do RGPD, o consentimento do aluno – que se supõe maior de idade - parece ser 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[55], e cumpridos os princípios relativos ao tratamento de dados pessoais (artigo 5.º *ibid.*).

O consentimento deve ser efetivamente livre, sem prejuízo do dever de ser também ele expresso, específico, informado e revogável.

---

[53] 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.

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

[55] 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».

4.1.2 Tratamento por motivos de interesse público

Uma vez que os interesses prosseguidos pelas entidades públicas correspondem aos interesses públicos (determinados por lei), seria necessário verificar-se essa prorrogativa legal.

No caso das instituições de ensino superior ministrado à distância, o disposto no art.º 14.º do Decreto-Lei n.º 133/2019, de 3 de setembro, reconhece a possibilidade de utilização de plataformas eletrónicas para efeito da avaliação à distância, exigindo que assegurem a viabilidade da avaliação.

Já no que concerne às restantes instituições 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 competentes de cada estabelecimento de ensino superior. Desta forma, seria suficiente a previsão dos modelos, de avaliação em tempo real ou com recurso à gravação, nas respetivas normas e regulamentos de avaliação das instituições, bem como a publicação do respetivo despacho reitoral de homologação[56].

O responsável pelo tratamento deve adotar as medidas necessárias para mitigar os riscos associados à gravação (na monitorização com recurso à gravação de vídeo), e à possibilidade de a mesma se verificar (ainda que na monitorização em tempo real). Entende-se que seria útil a aprovação de um código de conduta destinado aos vigilantes, que contribuísse para uma atividade idónea e limitada às finalidades da recolha dos dados. Por outro lado, teria que estar definido um prazo de conservação dos vídeos, bem como implementado um registo de acesso aos mesmos.

4.2 Monitorização automática e o tratamento de dados biométricos

No tradicional processo de vigilância dos alunos – em regime presencial -, a integridade e credibilidade de quem vigia as provas, por regra docentes, contribui diretamente para a aceitação do processo.

Quando o mesmo é automatizado, a integridade e a credibilidade do processo passam a depender do designer da tecnologia - das soluções existentes no estado da arte e adotadas nessa tecnologia - incluindo os programadores [DAVID, Nuno], estando ainda sujeitas a interferências externas (*e.g.* utilização de bibliotecas aplicacionais ou tecnologias obsoletas, exposição do repositório de código aplicacional a vulnerabilidades passíveis de serem exploradas). A credibilidade está, ainda, dependente de resultados fiáveis e, portanto, subordinada à implementação de funcionalidades que se revelem eficazes na deteção de fraude, para as quais a tecnologia de IA prestou um valioso contributo.

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

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[57]. De uma análise *prima facie* ao Considerando n.º 51 do RGPD, poderá entender-se que o tratamento de fotografias "processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular" constitui um tratamento de dados biométricos merecedor de específica proteção e, portanto, enquadrado no tratamento de categoriais especiais de dados pessoais[58]. Sabemos, porém, que 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, o n.º 1 do art.º 9 é perentório na proibição de tratamento dados biométricos (apenas) "para identificar uma pessoa de forma inequívoca".

Para clarificar a diferença entre os conceitos de identificação e de verificação ou autenticação biométricas reportamo-nos ao Parecer n.º 3/2012 do WP29[59] (p.6)[60] sobre a evolução das tecnologias biométricas, de onde se extrai, sobre a dentificação 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»)", definição que vai de encontro com a posição da Comissão Europeia, assumida no Livro Branco sobre a inteligência artificial (p.24)[61] e no qual

[57] 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."

[58] De acordo com n.º 1 do art.º 9.º do RGPD, dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. A redação reflete a preocupação relativamente aos dados biométricos para identificar uma pessoa de forma inequívoca, facto que não se encontrava vertido no art.º 6.º da Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (Convenção 108).

[59] Grupo de trabalho europeu, independente, 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 grupo substituído pelo *European Data Protection Board* (EDPB), ou Comité Europeu para a Proteção de Dados (CEPD).

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

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

se refere que "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".

Este 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 referida base de dados, e daí a necessidade de comparação com os vários modelos biométricos que constituem essa base de dados. Parece assim adequar-se às verificações efetuadas, por exemplo, no âmbito da base de dados de perfis de ADN para fins de identificação civil e criminal[62], ou ainda, na identificação para controlo de assiduidade ou de acesso a instalações.

Relativamente à verificação (ou autenticação) biométrica, refere o mesmo Parecer 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 modelo biométrico armazenado num dispositivo (ou seja, um processo de correspondência «um para um»)", referindo o Livro Branco sobre a inteligência artificial, tratar-se da "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 poderemos considerar o processo de verificação biométrica presente num *smartphone,* quando o seu proprietário configura o equipamento para que desbloqueie após verificação de uma imagem sua, recolhida em cada momento, face ao modelo biométrico criado no momento da configuração daquela funcionalidade.

Da interpretação direta dos conceitos, resultaria que o tratamento de dados biométricos deveria ser considerado enquanto categoria especial de dados pessoais apenas nos casos de identificação biométrica (comparação de um-para-um) e não nos casos de verificação (ou autenticação) biométrica (comparação de um-para-muitos).

[62] Cuja criação foi aprovada pela Lei n.º 5/2008, de 12 de fevereiro.

Não obstante, haverá que considerar que as soluções comerciais de monitorização automática garantem a validação da identidade do aluno, não só através de técnicas de reconhecimento facial, mas também por via do tratamento de outros dados biométricos já referidos, como sendo o padrão de escrita do aluno[63], ou dados comportamentais, que contribuem igualmente para o grau de sucesso da sua identificação. Por outro lado, não só efetuam a comparação dos dados biométricos no momento que antecede a prova, mas também durante o período da sua realização, no qual são capturadas novas imagens que, por sua vez, podem ter a dupla finalidade de servir para comparação imediata, mas ainda, para a partir delas se aperfeiçoar ou criar novos modelos biométricos para comparações futuras. A título de exemplo, a solução WISEflow, da UNIwise, permite configurar um período de retenção dos dados para identificação do aluno, incluindo novas fotografias para comparação futura e, portanto, novos modelos biométricos. Comparações posteriores à primeira passam, assim, de 'um-para-um' para 'um-para-muitos'. Já relativamente à solução *Respondus*, esse período é geralmente de cinco anos[64], a menos que seja contratualmente alterado.

Assim, entende-se que as soluções de monitorização automática deverão, à partida, ser abordadas na perspetiva do tratamento de categorias especiais de dados pessoais[65], requerendo a verificação de uma das exceções previstas no n.º 2 do artigo 9.º do RGPD.

4.2.1 Consentimento explícito do titular dos dados

À semelhança do exposto nos processos de monitorização não automáticos, entende-se que o consentimento do titular – sob as condições já referidas – seria igualmente válido para o tratamento de dados biométricos.

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. 9.º do RGPD. No entanto, o fundamento referido não só requer só 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.

---

[63] Como sucede com a solução *Respondus Monitor*.
[64] Cf. disponível em: <*https://support.respondus.com/hc/en-us/articles/4409595425307-How-long-is-video-kept-What-if-we-need-a-longer-period->.
[65] Note-se que, se assim não entender o responsável pelo tratamento, mas mantiver reservas, tem a obrigação de adotar a interpretação mais favorável à proteção dos direitos dos titulares.

Atentos no art.º 14.º, do Decreto-Lei n.º 74/2006, de 24 de março, a autonomia do respetivo órgão legal e estatutariamente competente para aprovar o regime de avaliação de conhecimentos não será preceito suficiente para permitir a utilização de técnicas de reconhecimento facial nos processos de avaliação.

Pelo facto de o tratamento incidir sobre categorias especiais de dados pessoais, sendo suscetível de provocar maior risco de ingerência nos direitos fundamentais[66] dos alunos, será necessário estatuir, sob a forma de diploma legal, em que medida e circunstâncias, pode a identificação dos estudantes, por recurso aos seus dados biométricos, ser justificada como interesse público 'importante' (Considerando 52 do RGPD).

Este parece ser, aliás, o caminho adequado, quando em causa esteja a restrição de direitos fundamentais dos titulares, uma vez que o Considerando 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)[67] permite ao responsável pelo tratamento - em princípio a instituição de ensino, a menos que essa responsabilidade seja (explicitamente) partilhada – não só avaliar a necessidade e proporcionalidade do tratamento dos dados, como ainda, auxiliá-lo na gestão dos riscos inerentes. Tem, portanto, uma dupla finalidade.

5.1 Tratamento de dados nos processos de monitorização não automáticos

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

[66] 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 EU), 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.
[67] Cujo conteúdo mínimo se encontra descrito no n.º 7 do art.º 35.º do RGPD.

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, 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[68], sendo óbvia, nesse caso, a necessidade de realizar uma AIPD.

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, por outro, se continuasse a permitir a utilização de versões obsoletas e inseguras[69].
A comercialização no mercado negro, de soluções 'chave na mão' para aceder remotamente a dispositivos vulneráveis é uma realidade[70] atual, sendo inclusive utilizada por instituições governamentais de vários países.

---

[68] Por referência ao Acórdão do TJUE, de 16 de julho de 2020, no processo C-311/18 (Acórdão *Schrems II*).
[69] 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>.*
[70] PERLROTH, Nicole, *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race,* Bloomsbury Publishing, 2021

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 à distância, e mais tarde a realização de provas de avaliação, não pode deixar de aqui se referir que poderia ter ido mais além na definição contratual dos já aqui referidos 'Termos de Utilização' do Colibri/Zoom, destacando-se, desta vez, a secção 15 relativa à 'Ausência de Garantias'[71] e a secção 17, relativa 'Limitação de Responsabilidade'[72], 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[73].

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 maior ou menor número de funcionalidades, a utilização de novas tecnologias[74] sempre será suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados.

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 implicando o tratando de categorias especiais de dados pessoais, automaticamente se exclui o n.º 10, já que o mesmo incide sobre específicos

[71] 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*>.

[72] 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].

[73] 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*>.

[74] Cf. n.º 1 do art.º 35.º do RGPD.

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 que a decisão final de anular ou não 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[75] 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 por base a reflexão efetuada, resumem-se, de seguida, os fundamentos de licitude adequado e a necessidade de realiza AIPD, em função de cada uma das categorias de monitorização descritas.

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. 6.º do RGPD, conjugada com a alínea g) do n.º 2 do artigo 9.º do mesmo diploma Ou Alínea a) do n.º 1 do art. 6.º do RGPD, conjugada com a alínea a) do n.º 2 do artigo 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

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

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 do tratamento de dados, incluindo, dos dados efetivamente tratados. Tal facto não favorece nem as instituições de ensino, que procuram no mercado as soluções capazes de responder às suas necessidades, nem os alunos, que procuram respostas cabais no momento em que se vêm confrontados com a necessidade de utilizar determinada solução de monitorização.

Determinadas soluções de monitorização possuem uma variedade de funcionalidades, de cuja utilização faz depender 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 os tratamentos de dados pessoais que realizam, respeitam os princípios e as regras legais de proteção dos dados[76].

Por outro lado, apesar de se ter demonstrado 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 na prossecução dos interesses (públicos) da instituição de ensino, mas também, nas situações em que o titular dá o seu consentimento para tratamento dos dados.

Em suma, e de acordo com as Orientações da CNPD[77], "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[78]". Não seria, portanto, razoável que por via do recurso à monitorização da avaliação à distância, pretendesse o responsável pelo tratamento, assegurar adicionais garantias, face às observadas em regime presencial.

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

[76] Nos termos do n.º 2 do art.º 5.º do RGPD.
[77] "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*>.
[78] Cf. alínea c) do n.º 1 do artigo 5.º do RGPD.

secundário, que possibilita a captação, de outra perspetiva, do local em que se 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, que lhe permitem configurar um ambiente de avaliação à distância fiável, em função das suas reais necessidades e do respeito pela privacidade dos titulares.

26