

INTELIGÊNCIA ARTIFICIAL: DOS SISTEMAS PROIBIDOS AOS DE ELEVADO RISCO

ARTIFICIAL INTELLIGENCE: FROM PROHIBITED SYSTEMS TO HIGH RISK SYSTEMS

Mário Frota¹

RESUMO

Para além do conceito de Inteligência Artificial em que assenta o Regulamento, o artigo caracteriza o risco, como pedra angular da disciplina que nele se estabelece, e procede à classificação dos sistemas sob uma tal perspectiva. Mas contempla tão só os sistemas de risco inaceitável e, por conseguinte, proibidos e os de risco elevado, que enuncia. E, dentre os sistemas proibidos, elege o ‘reconhecimento facial através da recolha aleatória de imagens a partir da Internet ou de televisão em circuito fechado’, a ‘inferência de emoções de uma pessoa natural no local de trabalho e nas instituições de ensino’, a ‘categorização biométrica para classificação individual de pessoas naturais com base em dados biométricos e a ‘identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública’, com particular enfoque nas suas peculiaridades; assim como, no que tange aos de elevado risco, destaca os sistemas de identificação biométrica à distância, os que aferem a categorização biométrica, de acordo com atributos ou características sensíveis ou protegidos com base na inferência de tais atributos ou características e os concebidos em ordem ao reconhecimento de emoções. E analisa as regras que no Regulamento se vertem sobre cada um dos sistemas.

PALAVRAS-CHAVE: Inteligência Artificial – Risco – Classificação do Risco - Risco Mínimo – Risco Limitado – Risco Elevado – Risco Inaceitável – Dados biométricos – Reconhecimento Facial – Identificação biométrica – Categorização biométrica – Reconhecimento de emoções -

RESUMEN

Además del concepto de Inteligencia Artificial en el que se basa el Reglamento, el artículo caracteriza el riesgo como piedra angular de la disciplina que se establece en él, y procede a clasificar los sistemas desde dicha perspectiva. Sin embargo, solo incluye los sistemas de riesgo inaceptables y, por tanto, prohibidos, así como los sistemas de alto riesgo que establece. Y, entre los sistemas prohibidos, elige el «reconocimiento facial mediante la recogida aleatoria de imágenes de Internet o de un circuito cerrado de televisión», la «inferencia de emociones de una persona física en el lugar de trabajo y en las instituciones educativas», «la categorización biométrica para la clasificación individual de personas físicas basada en datos biométricos» y la «identificación biométrica a distancia en "tiempo real" en espacios de acceso público con el fin de mantener la Orden público, con especial atención a sus peculiaridades; Así como, en lo que respecta a los de alto riesgo, destaca los sistemas de identificación biométrica remota, los que evalúan la categorización biométrica en función de atributos o características sensibles o

¹ Antigo Professor da Universidade de Paris Est. Fundador e primeiro presidente da AIDC – Associação Internacional de Direito do Consumo. Fundador e presidente emérito da apDC – de Direito do Consumo – Portugal.

protegidas a partir de la inferencia de dichos atributos o características, y los diseñados para el reconocimiento de emociones. Y analiza las reglas que se establecen en el Reglamento sobre cada uno de los sistemas.

PALABRAS CLAVE: Inteligencia Artificial – Riesgo – Clasificación de Riesgo – Riesgo Mínimo – Riesgo Limitado – Alto Riesgo – Riesgo Inaceptable – Datos Biométricos – Reconocimiento Facial – Identificación Biométrica – Categorización Biométrica – Reconocimiento de Emociones –

I

PRELIMINARES

1. Conceito de Inteligência Artificial

Por Inteligência artificial (IA) se concebe, em geral, os sistemas lógicos de programação que conferem às máquinas a capacidade de desempenhar funções como aprender, raciocinar e tomar decisões sobre as vias a seguir, de forma encadeada, consequente, ante determinadas situações.

A fórmula em que se baseia a Inteligência Artificial arranca da soma de mega-dados e da computação em nuvem e de adequados modelos de dados, cujo resultado conflui ou concorre para a concepção de máquinas mais ‘inteligentes’.

O conceito constante do Regulamento, com o no seu preâmbulo se previne, há que definir-se de forma inequívoca, estreitamente alinhado com o labor desenvolvido pelas organizações internacionais particularmente activas neste domínio, a fim de propiciar a segurança jurídica, facilitar a convergência global e a sua mais ampla aceitação, imprimindo-lhe em simultâneo a flexibilidade suficiente para se adaptar a rápidas evoluções tecnológicas observadas em um tal congenho.

Além disso, deverá basear-se nas principais características dos sistemas de IA que o distinguem de sistemas de *software* ou de abordagens de programação tradicionais mais simples e não deverá abranger sistemas baseados nas regras definidas exclusivamente por pessoas naturais para executarem operações automaticamente.

Uma característica principal dos sistemas de IA é a sua capacidade de proceder a inferências: o que decorre do processo de obtenção de resultados, tais como previsões, conteúdos, recomendações ou decisões susceptíveis de influenciar ambientes físicos e virtuais, e à capacidade dos sistemas de IA para obter modelos e/ou algoritmos a partir de entradas ou de dados.

As técnicas que permitem inferências durante a construção de um sistema de IA incluem abordagens de aprendizagem automática que ‘assimilam’ com os dados a forma de alcançar determinados objectivos, e outras baseadas na lógica e no conhecimento que operam inferências a partir do conhecimento codificado ou da representação simbólica da tarefa a resolver.

A capacidade de um sistema de IA de proceder a inferências vai além do tratamento básico de dados e permite a aprendizagem, o raciocínio ou a modelização.

O termo "baseado em máquinas" refere-se ao facto de os sistemas de IA funcionarem em máquinas.

A referência a objectivos explícitos ou implícitos visa sublinhar que os sistemas de IA podem funcionar de acordo com objectivos expressamente definidos, os explícitos, ou com os implícitos: os objectivos do sistema de IA podem ser diferentes da finalidade para tal prevista em um contexto específico.

Por "ambientes" se entende os contextos em que os sistemas de IA operam, ao passo que os resultados gerados pelo sistema de IA reflectem diferentes funções desempenhadas por tais sistemas e incluem previsões, conteúdos, recomendações ou decisões.

Os sistemas de IA são concebidos para operar com diferentes níveis de autonomia, o que significa que têm um certo grau de independência das acções efectuadas por intervenção humana e de capacidade para funcionar sem uma tal intervenção.

A capacidade de adaptação que um sistema de IA poderá apresentar após a implantação refere-se à capacidades de auto-aprendizagem, permitindo que o sistema mude enquanto se achar em funcionamento.

Os sistemas de IA podem ser utilizados autonomamente ou como componentes de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem nele estar incorporado (não integrado).

O Sistema de I.A., de harmonia com o que conceitua o Regulamento, é, pois, o sistema baseado em máquinas concebido para operar com vários níveis de autonomia e que pode, em relação a objectivos explícitos ou implícitos, criar resultados, como previsões, recomendações ou decisões, que influenciem ambientes físicos ou virtuais.

“A inteligência artificial é uma família de tecnologias em rápida evolução, capaz de oferecer - e decerto já oferece - um vasto conjunto de benefícios económicos, ambientais e sociais a todo o leque de indústrias e actividades sociais, se desenvolvida de acordo com princípios gerais pertinentes em conformidade com a Carta e com os valores em que a União Europeia se alicerça.”

Ao aperfeiçoar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais dispensadas às pessoas e às organizações, a inteligência artificial pode conferir importantes vantagens competitivas às empresas e contribuir para o progresso social e ambiental, por exemplo, nos cuidados de saúde, na agricultura, na segurança alimentar, na educação e na formação, nos meios de comunicação social, no desporto, na cultura, na gestão das infra-estruturas, na energia, nos transportes e logística, na gestão de crises, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos, na monitorização do ambiente, na preservação e recuperação da biodiversidade e dos ecossistemas e na atenuação das alterações climáticas e sua adaptação.

2. O risco como pedra angular dos sistemas de Inteligência Artificial

O princípio da precaução norteia o regime que o Regulamento Europeu, aprovado no Parlamento a 13 de Março pretérito, em co-decisão do Conselho da União Europeia, delineia para vigorar no lapso de dois anos após o vigésimo dia subsequente ao da sua publicação no Jornal Oficial (JOUE).

E, na apreciação dos sistemas e modelos, o *risco* assume relevante papel, dir-se-ia, uma posição nodular, nuclear.

E, na noção que dele traça, no glossário, o Regulamento, "risco" é a combinação da probabilidade de ocorrência de danos com a gravidade desses danos", com a gravidade que deles emana ou neles radica.

Os riscos, segundo a gravidade que lhes subjaz, definem-se por categorias a que quadra distinta disciplina ora traçada de modo inequívoco no Regulamento Europeu.

Eis as distintas categorias de riscos ali desenhadas:

- Inaceitáveis e, por conseguinte, proibidos,
- Elevados,
- Limitados e
- Mínimos

Por forma a que o complexo de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, há que adoptar uma abordagem baseada no risco claramente definida, como preambularmente se previne,

Para o efeito haverá que adaptar o tipo e o conteúdo normativo à intensidade e à janela de riscos susceptíveis de ser gerados pelos sistemas sob análise.

Daí que se torne imperioso regrar, a tempos e modos variáveis, a intensidade das medidas que se impuser se adoptem em função dos riscos perspectiváveis ou susceptíveis de concretização.

Conquanto a abordagem fundada no risco constitua a base para um conjunto proporcionado e eficaz de regras imperativas, importa não descurar, no entanto, as Directrizes Éticas para uma IA de Confiança, elaboradas em 2019 pelo GPAN / IA Independente designado para o efeito pela Comissão Europeia ⁽²⁾

² Sete os princípios éticos não vinculativos, ou seja, que não obrigam e se destinam a garantir uma IA de confiança e em consonância com a principiologia estruturalmente assente. Conquanto, pela disposição infra, pareça configurarem-se como oito e, não, sete.

Ei-los:

- ☐ Iniciativa e supervisão por humanos;
- ☐ Solidez técnica e segurança;
- ☐ Privacidade e governação dos dados;

-
- ☐ Transparência;
 - ☐ Diversidade,
 - ☐ Não discriminação e equidade;
 - ☐ Bem-estar social e ambiental e
 - ☐ Responsabilização.

Em simbiose com as normas emergentes de outros sistemas de valor, tais directrizes concorrem para a concepção de uma IA coerente, de confiança e centrada no ser humano, em consonância com a Carta de Direitos Fundamentais da União Europeia e com os princípios e valores em que a União Europeia se funda.

De harmonia com o guião exibido com a chancela do GPAN em IA,

- ☐ "iniciativa e supervisão por humanos": todos os sistemas de IA se desenvolvem e empregam como uma ferramenta ao serviço das pessoas, da dignidade humana e da autonomia pessoal, funcionando de molde a poder ser adequadamente controlada e supervisionada por humanos.
- ☐ "Solidez técnica e segurança": os sistemas de IA desenvolvem-se e empregam-se de forma a permitir solidez se decorrerem de problemas e resiliência contra tentativas de alteração do seu *modus faciendi* ou desempenho ao alcance do uso ilícito por terceiros, e de molde a minorar danos não intencionais susceptíveis de ocorrer.
- ☐ "Privacidade e governança dos dados": os sistemas de IA desenvolvem-se e empregam-se em conformidade com as disposições vertidas em tema de privacidade e de protecção de dados, ao mesmo tempo que o tratamento de dados satisfaz normas elevadas em termos de qualidade e de integridade.
- ☐ "Transparência": os sistemas de IA desenvolvem-se e empregam-se de molde a permitir uma rastreabilidade e explicabilidade adequadas, sensibilizando em simultaneidade os seres humanos para o facto de estarem a comunicar ou a interagir com um sistema de IA, informando devidamente os responsáveis pela implantação das capacidades e limitações de um tal sistema de IA e esclarecendo as pessoas afectadas dos direitos que lhes assistem.
- ☐ "Diversidade, não discriminação e equidade": os sistemas de IA desenvolvem-se e empregam-se de forma a incluir diferentes intervenientes e a promover a igualdade de acesso, a igualdade de género e a diversidade cultural, evitando em simultaneidade efeitos discriminatórios e enviesamentos injustos proibidos pelo direito da União ou pelas normas do direito nacional.
- ☐ "Bem-estar social e ambiental": os sistemas de IA desenvolvem-se e empregam-se de forma sustentável e em absoluto respeito pelo ambiente, intentando beneficiar os seres humanos, estimando ao mesmo tempo os impactos de longo prazo nas pessoas, na sociedade e no sistema democrático, nas suas distintas modelações. A aplicação de tais princípios deverá traduzir-se, sempre que possível, na concepção e na utilização de modelos de IA. Em qualquer caso, deverão servir de base para a elaboração de códigos de conduta ao abrigo das prescrições do actual regulamento. Incentiva-se as partes interessadas (indústria, academia, sociedade civil e instituições de normalização) a perfilhar, consoante o caso, os princípios éticos para o desenvolvimento de boas práticas e a adopção de normas voluntárias cuja observância inapelavelmente se impõe.
- ☐ "Responsabilidade": a capacidade de avaliação das próprias habilidades e acções e as possíveis consequências das decisões de molde a agir por forma a que os objectivos esperados tenham maior probabilidade de se alcançarem sem causarem danos de qualquer espécie na esfera seja de quem for.

É sobre o risco que se alicerça a análise, é sobre o risco que se edifica o sistema, consoante o seu teor e a sua natureza, a sua intensidade e o seu pendor.

3. A classificação segundo o risco oferecido pelos sistemas de Inteligência Artificial

Segundo o Regulamento em apreciação, os sistemas definir-se-ão segundo os riscos associados e a disciplina susceptível de lhe quadrar será proporcional à gravidade dos riscos que se antevêm ou se perspectivam.

3.1. Risco mínimo

O **risco mínimo** é o que subjaz à generalidade dos sistemas de inteligência artificial, desenvolvidos e empregues com observância da legislação que vigorará, sem que se estabeleçam obrigações jurídicas adicionais: a larga maioria dos sistemas de IA ora adoptados na UE - ou susceptíveis de o serem - insere-se em uma tal categoria ⁽³⁾

Os fornecedores dos sistemas podem optar por aplicar, na vertente hipótese, os requisitos para uma inteligência artificial fiável e aderir a códigos de conduta (códigos de práticas como ora se denominam no texto), de sua natureza facultativos, como o sugere o Regulamento no seu artigo 56.

Ao Serviço para a IA se comete a faculdade de “convidar todos os fornecedores de modelos de IA de finalidade geral, bem como as autoridades nacionais competentes, a participar na elaboração de códigos de práticas: as organizações da sociedade civil, a indústria, o meio académico e outras partes interessadas pertinentes, tais como fornecedores a jusante e peritos independentes”, poder-se-ão co-envolver na iniciativa e concorrer para a consecução de um tal propósito, a todos os títulos, relevante e meritório.

O Serviço para a IA e o Comité procurarão assegurar que os códigos de conduta definam claramente os objectivos específicos a que tendem e neles se inscrevam compromissos ou medidas, em que se incluem, se adequado, os indicadores-chave de desempenho, para garantir a consecução de um tal escopo, ponderando interesses e necessidades de todos os partícipes, neles figurando necessariamente as pessoas afectadas, no seio da União.

3.2. Risco limitado

Em uma tal categoria se inserem os sistemas cujo risco específico em matéria de transparência é patente e abrange determinados sistemas de inteligência artificial a que são impostos exigentes requisitos de transparência, *verbi gratia* quando haja um risco manifesto de manipulação (como

³ As aplicações de risco mínimo, a saber, os sistemas que formulam recomendações ou os filtros de correio electrónico não solicitado (vulgo, SPAM) com base na IA estarão isentos de quaisquer obrigações, uma vez que implicam um risco mínimo (quicá, nulo) para os direitos e a segurança dos cidadãos.

seja a utilização de sistemas de conversação automática ou de robôs de comunicação susceptíveis de iludir os seus interlocutores).

Quem os utiliza deve estar ciente de que interage com uma máquina que não com um ser humano.

O Regulamento considera também neste particular os riscos sistémicos potencialmente associados a modelos de IA de finalidade geral, incluindo grandes modelos de IA generativa, susceptíveis de utilização em uma série de tarefas e que se acham na base de muitos sistemas de IA na UE.

Alguns dos modelos, como tal caracterizados, podem comportar riscos sistémicos se forem muito potentes ou largamente utilizados, a saber, podem provocar graves acidentes ou ser empregues ilícita e abusivamente para ciber-ataques de vasto alcance.

Uma legião de cidadãos poderá vir a ser afectada se um modelo do jaez destes propagar preconceitos nocivos em muitas das aplicações.

Os grandes modelos de IA generativa são um exemplo típico de um modelo de IA de uso geral, dado que permitem a geração flexível de conteúdos (como na forma de texto, áudio, imagens ou vídeo) que podem facilmente acomodar uma ampla gama de tarefas distintas.

3.3. Risco elevado

Assiste um número limitado de sistemas, com um potencial susceptível de afectar negativamente a segurança das pessoas ou o respeito dos seus direitos fundamentais.

Em um anexo do Regulamento Europeu, a lista de sistemas de IA de risco elevado susceptível de revisão por forma a ajustar-se à evolução que entretanto se vier a registar.

Trata-se de um modelo aberto que não dominado por um qualquer “*numerus clausus*”

Uma tal lista inclui de modo análogo componentes de segurança de produtos abrangidos por legislação sectorial emanada da União, considerados de risco elevado sempre que sujeitos a avaliação de conformidade por terceiros por força de uma tal legislação sectorial.

Como exemplos de sistemas de risco elevado se poderá configurar o de determinadas infra-estruturas críticas, *verbi gratia*, nos domínios da água, do gás e da electricidade; dispositivos médicos; sistemas adoptados para determinar o acesso a estabelecimentos de ensino ou para efeitos do recrutamento de pessoal docente ou não docente; ou certos sistemas usados nos domínios da aplicação da lei, do controlo das fronteiras, da administração da justiça e dos processos democráticos (como os sistemas electivos e a sua *praxis*).

Os sistemas de identificação biométrica, categorização biométrica e reconhecimento de emoções também se consideram, no quadro do Regulamento Europeu, de alto risco ou risco elevado.

3.4. Risco inaceitável

Abrange um conjunto muito limitado de utilizações particularmente nocivas de sistemas de IA que violam os direitos fundamentais ínsito na Carta da UE, donde a sua proibição, a saber, aplicações que manipulem o comportamento humano para iludir o livre arbítrio de quem os usa (v.g., brinquedos para menores com assistência de voz que encoraje comportamentos perigosos), sistemas que permitam uma «classificação social» por parte das administrações públicas ou das empresas e determinadas aplicações de policiamento ou vigilância baseadas em previsões.

Vedadas também se acham determinadas utilizações de sistemas biométricos, tais como os de reconhecimento de emoções no local de trabalho, de categorização social ou de identificação biométrica remota em tempo real para efeitos da aplicação da lei em espaços acessíveis ao público (com excepções contadas).

Os riscos que se têm por mais graves figuram – *et pour cause* – no *index* e são de todo de excluir, como aliás o faz percucientemente o Regulamento, alçado a instrumento de análise.

São, por conseguinte, proscritos determinados sistemas. Não se admitem de nenhum modo. Com ou sem precauções. Conquanto se registem restritíssimas excepções que em lugar próprio se constituirão em objecto de análise.

II

RISCO INACEITÁVEL:

PRÁTICAS ABSOLUTAMENTE PROIBIDAS

1. O Risco Inaceitável vedado imperativamente pelo Regulamento Europeu

Como se assinalou, por forma a que o complexo de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, há que adoptar uma abordagem baseada no risco claramente definida.

Para o efeito haverá que adaptar o tipo e o conteúdo normativo à intensidade e ao complexo de riscos susceptíveis de ser criados pelos sistemas em análise.

Daí que se torne imperioso proibir um sem-número de práticas inaceitáveis de IA.

Conquanto a abordagem fundada no risco constitua a base para um conjunto proporcionado e eficaz de regras imperativas, importa não ignorar, no passo de que se trata, as Directrizes Éticas para uma IA de Confiança, elaboradas em 2019 pelo GPAN em IA independente, nomeado em devido tempo pela Comissão Europeia.

Em tais directrizes se recortou um acervo de sete princípios éticos não vinculativos para a IA, cuja observância visa garantir, porém, sistemas de confiança e eticamente irrepreensíveis.

Como condição prévia, a IA erguer-se-á como tecnologia centrada no ser humano: servirá para tanto como instrumento para as pessoas, com o objectivo último de incrementar o bem-estar de cada um e de todos e das comunidades nacionais congregadas em redor do projecto sócio-económico em que radica a União Europeia.

Revelar-se-ão, ainda que de modo sintético, tais princípios, a saber: iniciativa e supervisão por humanos; solidez técnica e segurança; privacidade e governança dos dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental e consequente responsabilização.

Sem prejuízo dos requisitos juridicamente vinculativos que no Regulamento se conformam e de quaisquer outras disposições aplicáveis emergentes do direito da União, tais directrizes (*guidelines*), como preambularmente se assinala, contribuem para a concepção de uma IA coerente, de confiança e centrada e com enfoque no ser humano, em iniludível consonância com a Carta de Direitos Fundamentais da União Europeia e os valores em que se alicerça o edifício institucional deste relevante bloco regional.

2. A enunciação dos sistemas de “risco inaceitável” segundo o Regulamento Europeu: o estado da arte

O Regulamento, ora aprovado, prevê-os expressamente no n.º 1 do seu artigo 5.º, em obediência a um *numerus clausus* irrefragável.

Perspectivam-se e figuram como **riscos inaceitáveis** e, por conseguinte, proibidos *ex vi legis*, os que enformam sistemas que:

- ☐ Empreguem técnicas subliminares que contornem a consciência de uma pessoa ou que a manipulem manifestamente ou a ludibriem, com o objectivo ou o efeito de distorcer substancialmente o seu comportamento ou o de um grupo, afectando de forma considerável a sua capacidade de decisão;
- ☐ Explorem vulnerabilidades de uma pessoa ou de um grupo específico devido à idade, incapacidade ou situação sócio-económica, com o fito de distorcer substancialmente o seu comportamento ou de pessoa pertencente ao grupo de tal forma que cause ou seja razoavelmente susceptível de causar-lhe significativos prejuízos;
- ☐ Avaliem ou classifiquem pessoas naturais ou grupos de pessoas durante um certo período com base no seu comportamento social ou em características de personalidade, conhecidas, inferidas ou previsíveis, em que tal classificação social conduza a tratamento prejudicial ou desfavorável:
 - o em contextos sociais não relacionados com aqueles em que os dados foram originalmente gerados ou recolhidos;
 - o que seja injustificado ou desproporcionado face ao seu comportamento social ou à gravidade de que se reveste;

- Visem uma finalidade específica ou se adoptem para avaliação de risco de pessoas naturais a fim de aferir ou prever a probabilidade de virem a cometer uma infracção penal, com base exclusivamente numa definição de perfis ou na avaliação dos seus traços e características de personalidade (o que não se aplica aos sistemas que se destinem a apoiar a avaliação do envolvimento de uma pessoa em actividade criminosa, que se baseie já em factos objectivos e verificáveis, directamente ligados a tal);
- Criem ou expandam bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir da Internet ou de imagens de televisão em circuito fechado;
- Se destinem a inferir emoções de uma pessoa natural no local de trabalho e nas instituições de ensino, excepto se se destinar a ser instalado ou introduzido no mercado por razões médicas ou de segurança;
- Visem a categorização biométrica para classificação individual de pessoas naturais com base em dados biométricos para deduzir ou inferir a sua raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida ou orientação sexual (tal proibição não abrange rotulagens nem filtragens de conjuntos de dados biométricos legalmente adquiridos, tais como imagens, com base em dados biométricos ou na categorização de dados biométricos no domínio da manutenção da ordem pública);
- Se destinem a identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública, a menos e na medida em que tal utilização seja estritamente necessária para um dos seguintes fins:
 - o busca selectiva de vítimas específicas de rapto, tráfico ou exploração sexual de seres humanos, bem como a de pessoas desaparecidas;
 - o prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e actual ou real e previsível de um ataque terrorista;
 - o a localização ou identificação de uma pessoa suspeita de ter cometido uma infracção penal, para efeitos da realização de uma investigação criminal, instauração de acção penal ou execução de uma sanção penal por alguma das 16 infracções enunciadas em anexo e puníveis no Estado-membro de que se trate com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.

3. O enfoque sob dados parâmetros e sua consequente apreciação

Elegeremos, neste passo, o “reconhecimento facial através da recolha aleatória de imagens a partir da Internet ou de televisão em circuito fechado”, a “inferência de emoções no local de trabalho ou nas instituições de ensino”, a “identificação biométrica à distância em ‘tempo real’ em espaços acessíveis ao público para efeitos de manutenção da ordem pública” e “a categorização biométrica para classificação individual de pessoas naturais com base em dados biométricos”.

Apreciemos cada um de per si nos passos subsequentes,

1.1. Reconhecimento facial através da recolha aleatória de imagens a partir da Internet ou de televisão em circuito fechado

O conceito de "dados biométricos" deve ser interpretado à luz do que prescreve, entre outros, o Regulamento Geral de Protecção de Dados, a saber, “os 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 de uma tal pessoa, nomeadamente as imagens faciais ou os dados dactiloscópicos”.

Os dados biométricos podem permitir a autenticação, identificação ou categorização de pessoas singulares e o reconhecimento das suas emoções.

O que é o reconhecimento facial?

Algo que consiste num peculiar meio de identificar ou confirmar a identidade de uma pessoa natural através do rosto ou fâcies, susceptível de ser usado para identificar de modo diferido pessoas em fotos, vídeos ou, em simultaneidade, ‘em tempo real.’

Perspectiva-se o reconhecimento facial como uma categoria de segurança biométrica.

Outras modelações de *software* biométrico incluem, designadamente, o reconhecimento de voz, a impressão digital, a retina ocular ou a íris. A tecnologia é usada, em geral, para segurança e aplicação da lei, embora haja um interesse crescente em outros relevantes domínios que se abrem à sua exploração.

A pessoas, em geral, identificam a tecnologia de reconhecimento mercê do Face ID, usado para desbloquear o *iPhone*, como uma simples aplicação de reconhecimento facial.

Normalmente, o reconhecimento facial não conta com um amplo banco de dados de fotos para determinar a identidade de quem quer que seja; identifica simplesmente a pessoa de que se trata e reconhece-a como sendo a titular única do dispositivo, limitando o acesso aos mais.

Além de permitir o desbloqueamento de equipamentos celulares, o reconhecimento facial promove a correspondência entre os rostos de pessoas que se postam diante de câmaras especiais com as imagens que figuram em uma lista de observação. As listas disporão de imagens de qualquer pessoa, incluindo das que não sejam suspeitas de uma qualquer infracção; e as imagens podem ter origem, como se assinala, em um qualquer lugar, até mesmo das contas das redes sociais que são amplamente povoadas de registos do estilo.

Como se destaca do preâmbulo do Regulamento, no seu n.º 43, “a colocação no mercado ou em serviço para este fim específico ou a utilização de sistemas de IA que criem ou expandam bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais da Internet ou de imagens de CCTV deverão ser proibidas por esta prática aumentar o sentimento de

vigilância em larga escala e poder conduzir a violações grosseiras dos direitos fundamentais, incluindo o direito à privacidade.”⁽⁴⁾

O facto é que o Regulamento o proíbe, como se assinalou, considerando que o reconhecimento facial constitui uma categoria abrangida na dos “riscos inaceitáveis”.

1.2. Inferência de emoções de uma pessoa natural no local de trabalho e nas instituições de ensino

⁴ Como se inscreve in Kapersky, “O que é reconhecimento facial – definição e explicação”, abundam os exemplos do emprego do reconhecimento facial por empresas majestáticas, a saber,

“Antigamente, a Amazon incentivava o uso do seu serviço de reconhecimento facial baseado em nuvem, chamado Rekognition, por parte dos órgãos de aplicação da lei. No entanto, em uma postagem no blog da empresa em junho de 2020, a Amazon anunciou que estava planejando uma moratória de um ano no uso de sua tecnologia por parte da polícia. A razão por trás disso foi aguardar até que as leis federais dos EUA entrassem em vigor, para proteger os direitos humanos e a liberdade civil.

A Apple usa o reconhecimento facial para ajudar os usuários a desbloquear rapidamente seus telefones, fazer login em aplicativos e realizar compras.

A British Airways usa o reconhecimento facial para os passageiros embarcarem nos voos saindo dos EUA. É possível fazer a leitura facial dos passageiros e, conseqüentemente, verificar a identidade deles, usando uma câmara a bordo do avião sem que precisem mostrar o passaporte ou o cartão de embarque. A companhia aérea tem usado a tecnologia em voos dentro do Reino Unido saídos do aeroporto de Heathrow e está trabalhando para adotar o embarque biométrico em voos internacionais.

A Cigna, uma seguradora de saúde dos EUA, permite que os clientes na China emitam pedidos de seguro saúde onde a assinatura é uma foto, em vez de escrita, na tentativa de reduzir o número de fraudes.

A Coca-Cola tem usado o reconhecimento facial de várias formas no mundo todo. Entre os exemplos estão a recompensa de clientes que reciclam em algumas das máquinas de venda automática na China anúncios personalizados em máquinas de venda automática na Austrália e marketing de eventos em Israel.

O *Facebook* (Meta) começou a usar o reconhecimento facial nos EUA em 2010, quando marcava automaticamente pessoas nas fotos usando sua ferramenta de sugestão de marcação. A ferramenta faz a leitura facial de um usuário e oferece sugestões de quem essa pessoa é. Desde 2019, o Facebook tornou o recurso opcional como parte de um mecanismo mais focado na privacidade. Mais informações do *Facebook* (Meta) sobre como aceitar ou recusar o reconhecimento facial podem ser encontradas aqui.

O Google incorpora a tecnologia no Google Fotos e a utiliza para classificar as imagens e marcá-las automaticamente com base nas pessoas reconhecidas.

A MAC make-up usa a tecnologia de reconhecimento facial em algumas de suas lojas físicas, permitindo que os clientes praticamente “experimentem” a maquiagem com o uso de espelhos de realidade aumentada da loja.

O McDonald’s usa o reconhecimento facial em seus restaurantes no Japão para avaliar a qualidade do atendimento ao cliente, incluindo se seus funcionários estão sorrindo enquanto atendem.

O Snapchat é um dos pioneiros no uso de software de reconhecimento facial: com ele, marcas e organizações podem criar filtros que moldam o rosto do usuário; ou seja, filtros de cachorrinho e coroa de flores podem ser vistos na rede social.”

O conceito de "sistema de reconhecimento de emoções" define-se como um sistema de IA concebido para identificar ou inferir emoções ou intenções de pessoas naturais com base em seus dados biométricos.

O conceito encerra, como sói dizer-se, emoções ou intenções como a felicidade, a tristeza, a raiva, a surpresa, a repugnância, o embaraço, o entusiasmo, a vergonha, o desprezo, a satisfação e o divertimento.

O conceito, na acepção de que se trata, não inclui estados físicos, como dor ou fadiga; não se refere, v.g., aos sistemas adoptados para detectar o estado de fadiga dos pilotos ou motoristas profissionais em ordem à prevenção de acidentes.

Não inclui de análogo modo a mera detecção de expressões, gestos ou movimentos rapidamente visíveis, a menos que sejam utilizados para identificar ou inferir emoções.

Tais expressões podem ser designadamente gestos faciais básicos, como franzir a testa ou sorrir, ou gestos como o movimento das mãos, dos braços ou da cabeça, ou características da voz de uma pessoa, por exemplo, ao levantar a voz ou sussurrar.

O sistema de reconhecimento de emoções de pessoa natural no local de trabalho como nas instituições de ensino por virtude de comportar um risco inaceitável, como as excepções que se aduzem, proibido se acha, de harmonia com o que prescreve o Regulamento Europeu na alínea e) do n.º 1 do seu artigo 5.º

1.3. Categorização biométrica para classificação individual de pessoas naturais com base em dados biométricos

O conceito de ‘dados biométricos’ já o recortámos *supra* (em 3.1.).

O conceito de ‘sistema de categorização biométrica’ define-se como a atribuição ou a afectação de pessoas naturais a categorias específicas com base nos seus dados biométricos.

Tais categorias específicas são susceptíveis de convir a determinados características como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços comportamentais ou de personalidade, língua, religião, pertença a uma minoria nacional, orientação sexual ou política.

Tal não abrange, como o pretende o Regulamento, os sistemas de categorização biométrica que se traduzam em um elemento meramente acessório intrinsecamente ligado a um outro serviço comercial, o que significa que o elemento não pode, por razões técnicas objectivas, ser utilizado por si só, sem o serviço principal e a integração desse elemento ou funcionalidade não constitui um meio para contornar a aplicabilidade das regras ora constantes do normativo de que se trata.

Por exemplo, os filtros que categorizam as características faciais ou corporais utilizadas nos mercados em linha poderão constituir um desses elementos acessórios, uma vez que só podem ser utilizados associados ao serviço principal que consiste em vender um produto, ao facultarem ao consumidor a possibilidade de se pré-visualizar a usar o produto e ajudando-o a tomar uma decisão de compra. Os filtros utilizados nos serviços de redes sociais em linha que categorizam características faciais ou corporais para permitir que os utilizadores acrescentem ou alterem

imagens ou vídeos também poderão ser considerados elementos acessórios, uma vez que tais filtros não podem ser utilizados sem o serviço principal dos serviços da rede social, que consiste na partilha de conteúdos em linha.

Deverão ser proibidos os sistemas de categorização biométrica baseados em dados biométricos de pessoas naturais, como o rosto ou as impressões digitais, para deduzir ou inferir as suas opiniões políticas, a filiação sindical, as convicções religiosas ou filosóficas, a raça, a vida sexual ou a orientação sexual de uma pessoa.

Tal proibição, no entanto, não deverá abranger a rotulagem legal, a filtragem ou a categorização de conjuntos de dados biométricos adquiridos em conformidade com o direito da União ou o direito nacional em função dos dados biométricos, como a triagem de imagens em função da cor do cabelo ou da cor dos olhos, que podem, por exemplo, ser utilizadas no domínio da manutenção da ordem pública, sempre que por lei permitida.

1.4. Identificação biométrica à distância em "tempo real" em espaços acessíveis ao público para efeitos de manutenção da ordem pública

O conceito de "identificação biométrica" define-se como o reconhecimento automatizado de características humanas físicas, fisiológicas e comportamentais, tais como o rosto, o movimento dos olhos, a forma do corpo, a voz, a pronúncia, a marcha, a postura, a frequência cardíaca, a pressão arterial, o odor, as características da digitação, com o objectivo de verificar a identidade de uma pessoa comparando os dados biométricos dessa pessoa com dados biométricos de pessoas armazenados numa base de dados de referência, independentemente de a pessoa ter ou não dado consentimento prévio para o efeito..

Estão excluídos os sistemas de IA concebidos para verificação biométrica, o que inclui a autenticação, cujo único objectivo seja o de confirmar que uma dada pessoa singular específica é quem afirma ser, e confirmar a sua identidade com o único objectivo de ter acesso a um serviço, desbloquear um dispositivo ou ter acesso de segurança a um determinado local.

Sistemas de identificação biométrica à distância em "tempo real" em espaços acessíveis ao público ⁵ para efeitos de manutenção da ordem pública, a menos e na medida em que essa utilização seja estritamente necessária para um dos seguintes fins:

⁵ De harmonia com o Regulamento Europeu, há que explicitar de modo expresso o conceito de “espaço acessível ao público”, inerente à norma *sub judice*.

O entendimento do que seja "espaço acessível ao público" constrói-se a partir da noção de um qualquer espaço físico acessível a um número indeterminado de pessoas naturais e independentemente de um tal espaço ser detido por entidade pública ou privada, sem curar de saber da actividade para a qual se destine: por exemplo, comércio (designadamente lojas, estabelecimentos mercantis, centros comerciais, superfícies comerciais, micro, mini, super e hipermercados), serviços (designadamente instituições de crédito, sociedades financeiras, companhias de seguros, actividades desenvolvidas por profissionais liberais, serviços públicos fisicamente disponíveis ao público em geral), actividades de hotelaria e restauração, snacks, cafetarias, actividades desportivas (designadamente piscinas, ginásios, estádios), transportes (designadamente estações de autocarros, metropolitanos e gares ferroviárias, aeroportos, meios de transporte), entretenimento (designadamente cinemas, teatros, museus, salas de concertos e salas de conferências), lazer ou outros (designadamente estradas, praças, parques, florestas ou parques infantis públicos).

- i) busca selectiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca de pessoas desaparecidas;
- ii) prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e actual ou real e previsível de um ataque terrorista;
- iii) a localização ou identificação de uma pessoa suspeita de ter cometido uma infracção penal, para efeitos da realização de uma investigação criminal, instauração de acção penal ou execução de uma sanção penal por alguma das infracções referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos ⁶.

A identificação biométrica à distância em tempo real pelas autoridades responsáveis pela aplicação da lei estaria sujeita a autorização prévia de uma autoridade judicial ou administrativa independente cuja decisão seja vinculativa. Em caso de urgência, a autorização pode ser

Um local também deverá ser classificado como acessível ao público se, independentemente das eventuais restrições de capacidade ou de segurança, o acesso estiver sujeito a condições predeterminadas, susceptíveis de ser preenchidas por um número indeterminado de pessoas, tais como a compra de um bilhete ou título de transporte, a inscrição prévia ou restrito a uma determinada idade.

Em contrapartida, um local não deverá ser considerado acessível ao público se o acesso for limitado a pessoas naturais específicas e definidas, seja nos termos do direito da União ou do direito nacional directamente imbricado na segurança pública ou por manifestação clara da vontade de quem exerça a autoridade pertinente no local.

Outros espaços podem ser compostos por zonas não acessíveis ao público e por outras acessíveis ao público, tais como um corredor de um edifício residencial privado necessário para aceder a um gabinete médico ou a um aeroporto.

Os espaços em linha também não são abrangidos, uma vez que não são espaços físicos. Para determinar se um espaço é acessível ao público deverá recorrer-se a uma análise casuística, tendo em conta as especificidades da situação em apreço.

As instalações de empresas e fábricas, bem como os escritórios e os locais de trabalho a que se pretende que apenas os trabalhadores e prestadores de serviços pertinentes tenham acesso, são espaços não acessíveis ao público.

Os espaços acessíveis ao público não deverão incluir nem estabelecimentos de reclusão nem zonas de controlo fronteiriço.

A possibilidade factual de acesso por si só (como uma porta destrancada ou um portão aberto numa vedação) não implica que o espaço seja acessível ao público na presença de indicações ou circunstâncias que sugiram o contrário (como sinais que proibam ou restrinjam o acesso).

⁶ A lista de 16 crimes inclui:

- o Terrorismo;
- o Tráfico de seres humanos;
- o Exploração sexual de crianças e material pedopornográfico;
- o Tráfico de estupefacientes e substâncias psicotrópicas;
- o Tráfico de armas, munições e explosivos;
- o Homicídio voluntário;
- o Ofensas corporais graves;
- o Tráfico de órgãos e de tecidos humanos;
- o Tráfico de materiais nucleares e radioactivos;
- o Rapto, sequestro e tomada de reféns;
- o Crimes abrangidos pela jurisdição do Tribunal Penal Internacional;
- o Desvio de aeronaves ou navios;
- o Violação;
- o Criminalidade ambiental;
- o Roubo organizado ou à mão armada;
- o Sabotagem, participação numa organização criminosa envolvida num ou vários crimes acima enumerados.

concedida no prazo de 24 horas; se a autorização for rejeitada, todos os dados e resultados têm de ser apagados.

Teria de ser precedida de uma avaliação de impacto sobre os direitos fundamentais e notificada à autoridade de fiscalização do mercado competente e à autoridade de protecção de dados.

Em caso de urgência, a utilização do sistema pode ser iniciada sem o registo.

A utilização de sistemas de IA para a identificação biométrica à distância em diferido (identificação de pessoas em material vídeo previamente recolhido) de pessoas sob investigação exige autorização prévia de uma autoridade judicial ou de uma autoridade administrativa independente e a notificação da autoridade de protecção de dados e da autoridade de fiscalização do mercado.

III

RISCO ELEVADO

PRÁTICAS ESTRITAMENTE REGULAMENTADAS

1. Definição

Em paralelo com uma definição clara do conceito de «risco elevado», o Regulamento estabelece uma metodologia eficaz para ajudar a identificar tais sistemas ante o quadro jurídico estabelecido: o objectivo é o de proporcionar segurança jurídica às empresas e aos demais operadores.

A classificação de risco baseia-se na finalidade prevista do sistema de IA, em consonância com a legislação da UE vigente em matéria de segurança dos produtos: tal significa que a classificação de risco depende da função que o sistema de IA desempenha e das finalidades e modalidades específicas em que é empregue.

Em anexo (III) ao regulamento figura uma lista de sistemas considerados como de risco elevado.

A Comissão assegurará a actualização de uma tal lista, que não é, pois, nem exaustiva nem imune aos progressos (...) ou à evolução que entretanto se registar.

Os sistemas constantes da lista de risco elevado que executam tarefas processuais restritas, melhoram o resultado de actividades humanas anteriores, não influenciam decisões humanas ou realizam tarefas puramente preparatórias... não são considerados, pois, de risco elevado.

Todavia, convém reter que um sistema de IA deve ser sempre considerado de risco elevado se definir perfis de pessoas naturais (ou físicas).

Antes de colocarem sistemas de inteligência artificial de risco elevado no mercado da UE ou de os disporem ao seu serviço, os fornecedores terão de os sujeitar a uma avaliação da

conformidade. Tal permitir-lhes-á revelar que os sistemas cumprem os requisitos obrigatórios para uma inteligência artificial fiável (v. g., qualidade dos dados, disponibilidade de documentação e rastreabilidade, transparência, supervisão humana, exactidão, ciber-segurança e solidez): avaliação que tem de ser repetida se o sistema ou a sua finalidade forem substancialmente alterados.

A título de exemplo, refira-se que os sistemas de inteligência artificial que sejam componentes de segurança de produtos abrangidos por legislação sectorial da União serão considerados de risco elevado sempre que se destinem a servir de suporte a

- o Certas infra-estruturas críticas, por exemplo, nos sectores do tráfego rodoviário e do abastecimento de água, gás, aquecimento e electricidade;
- o Educação e formação profissional, por exemplo, para avaliar os resultados da aprendizagem, orientar o seu processo e acompanhar a fraude;
- o Emprego, gestão dos trabalhadores e acesso ao trabalho por conta própria, por exemplo, para colocar anúncios de emprego específicos, analisar e filtrar candidaturas de emprego e avaliar candidatos;
- o Acesso a serviços e benefícios públicos e privados essenciais (por exemplo, cuidados de saúde), avaliação da capacidade de endividamento de pessoas singulares e avaliação dos riscos e fixação de preços em relação a seguros de vida e de saúde;
- o Certos sistemas usados nos domínios da aplicação da lei, do controlo das fronteiras, da administração da justiça e dos processos democráticos.
- o Avaliação e classificação das chamadas de emergência;
- o Identificação biométrica, categorização biométrica e reconhecimento de emoções (excepto as categorias proibidas);
- o Os sistemas de recomendação de plataformas em linha de muito grande dimensão não estão incluídos, uma vez que se acham já abrangidos pelo Reg.to de Serviços Digitais, ou seja, o Regulamento 2022/2065, de 19 de Outubro de 2022

Ante os Sistemas de IA componentes da segurança de produtos ou eles mesmo como produtos na categoria de risco elevado, citem-se como frisantes exemplos com que, de resto, nos confrontamos no quotidiano:

Máquinas, brinquedos, ascensores, aparelhos e sistemas de protecção destinados a ser utilizados em atmosferas potencialmente explosivas, equipamentos de rádio, equipamentos sob pressão, equipamentos para embarcações de recreio, instalações por cabo, aparelhos de combustão de combustíveis gasosos, dispositivos médicos e dispositivos médicos para diagnóstico *in vitro*.

Devem estar sujeitos a avaliação da conformidade por terceiros por força da legislação sectorial. A avaliação da conformidade por terceiros é igualmente obrigatória para todos os sistemas biométricos.

Os fornecedores de sistemas de inteligência artificial de risco elevado terão também de pôr em prática sistemas de gestão da qualidade e dos riscos que garantam a sua conformidade com os novos requisitos e minimizem os riscos para os utilizadores e as pessoas afectadas, mesmo após a colocação do produto em causa no mercado.

Os sistemas de IA de risco elevado implantados por autoridades públicas ou entidades que actuam em seu nome terão de ser registados numa base de dados pública da UE, salvo se forem utilizados para fins de aplicação da lei e migração. Estes últimos terão de ser registados numa parte não pública da base de dados, a qual só será acessível às competentes autoridades de controlo.

As autoridades de fiscalização do mercado apoiarão o acompanhamento pós-comercialização, realizando auditorias e proporcionando aos fornecedores a possibilidade de comunicarem incidentes graves ou violações das obrigações em matéria de direitos fundamentais de que tenham conhecimento.

Qualquer autoridade que opere funcionalmente na fiscalização do mercado pode autorizar a colocação no mercado de IA de risco elevado específica por motivos excepcionais.

Os requisitos permitirão que, em caso de infracção, as autoridades nacionais acedam às informações necessárias por forma a investigar se a utilização do sistema de inteligência artificial observou estritamente os ditames da lei.

2. Modalidades

Num dos anexos do Regulamento (o III), como se registou, se compendiam os sistemas de Inteligência Artificial classificados como de ‘Risco Elevado’ ante as características de que se revestem, tal como emergem do n.º 2 do seu artigo 6.º:

Ei-los:

- 2.1.** Dados biométricos cujo emprego se permita ao abrigo do direito da União ou do ordenamento pátrio aplicável:
 - (i) Sistemas de identificação biométrica à distância (em que se não incluem os sistemas de IA concebidos em ordem à verificação biométrica com o único propósito de confirmar que uma determinada pessoa singular é quem alega ser;
 - (ii) Sistemas de IA concebidos de molde a que se afira a categorização biométrica, de acordo com atributos ou características sensíveis ou protegidos com base na inferência de tais atributos ou características;
 - (iii) Sistemas de IA concebidos em ordem ao reconhecimento de emoções.
- 2.2.** Infra-estruturas críticas:
 - (i) Sistemas de IA concebidos de molde a utilizarem-se como componentes de segurança na gestão e no controlo de infra-estruturas digitais críticas, do trânsito rodoviário ou das redes de abastecimento de água, gás, aquecimento ou electricidade.

2.3. Educação e formação profissional:

Sistemas de IA concebidos em ordem a

- (i) Determinar o acesso ou a admissão ou a afectação de pessoas singulares a instituições de ensino e de formação profissional de todos os níveis;
- (ii) Avaliar os resultados da aprendizagem, nomeadamente quando tais resultados se usam para orientar o processo de aprendizagem de pessoas singulares em instituições de ensino e de formação profissional de todos os níveis;
- (iii) Avaliar o nível de educação adequado que as pessoas receberão ou a que poderão ter acesso no contexto de instituições de ensino e formação profissional ou a tais instituições;
- (iv) O controlo e detecção de práticas proibidas por parte de estudantes durante os testes no contexto de instituições de ensino e formação profissional ou em tais instituições.

2.4. Emprego, gestão de trabalhadores e acesso ao emprego por conta própria:

- (i) Sistemas de IA concebidos por forma a que se empreguem no recrutamento ou na selecção de pessoas singulares, em especial para colocação de anúncios de emprego direccionados, análise e triagem de candidaturas a ofertas de emprego e avaliação dos candidatos;
- (ii) Sistemas de IA concebidos de molde a tomarem decisões que afectem os termos das relações de trabalho, a promoção ou a cessação das relações contratuais de trabalho, na atribuição de tarefas com base em comportamentos individuais, traços ou características pessoais, ou no controlo e avaliação do desempenho e da conduta de pessoas que são partes em tais relações.

2.5. Acesso a serviços públicos ou privados essenciais e a prestações públicas de análoga natureza, bem como o seu desfrute:

- (i) Sistemas de IA concebidos para ser empregues por autoridades públicas, ou em seu nome, para avaliar a elegibilidade de pessoas singulares no acesso a prestações e serviços de assistência pública essenciais, incluindo cuidados de saúde, bem como para conceder, reduzir, revogar ou recuperar o acesso a tais prestações e serviços;
- (ii) Sistemas de IA concebidos para ser empregues na avaliação da solvabilidade de pessoas singulares ou no estabelecimento da sua classificação de crédito, com excepção dos sistemas de IA para efeitos de detecção de fraude financeira;

- (iii) Sistemas de IA concebidos para ser empregues nas avaliações de risco e na fixação de preços em relação a pessoas singulares no caso de seguros de vida e de saúde;
- (iv) Sistemas de IA concebidos para avaliação e classificação de chamadas de emergência efectuadas por pessoas singulares ou para serem usados no envio, ou no estabelecimento de prioridades no envio, de serviços de primeira resposta a emergências, incluindo polícia, bombeiros e assistência médica, bem como sistemas de triagem de pacientes dos sistemas de cuidados de saúde de emergência;

2.6. Manutenção da ordem pública, na medida em que a sua utilização se permita, nos termos do direito da União ou do direito nacional aplicável:

Em causa sistemas de IA concebidos para utilização por autoridades a quem incumba a aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União Europeia (ou em apoio de tais autoridades)

- (i) para avaliação do risco de uma pessoa singular poder vir a ser vítima de uma qualquer infracção penal;
- (ii) como polígrafos ou instrumentos semelhantes;
- (iii) para avaliação da fiabilidade dos elementos de prova no decurso de uma investigação ou de acção penal relativa a infracções de uma tal natureza;
- (iv) para avaliação da probabilidade de uma pessoa singular cometer uma infracção penal ou reincidir não exclusivamente com base na definição de perfis de pessoas singulares (nota) (nota: na acepção do artigo 3.º, ponto 4, da Directiva (UE) 2016/680), ou para avaliação dos traços e características de personalidade ou do comportamento criminal pretérito tanto de pessoas singulares como de grupos;
- (v) para definição do perfil de pessoas singulares na acepção a que se alude precedentemente, no decurso da detecção, investigação ou acção relativa a uma qualquer infracção penal.

2.7. Gestão da migração, do asilo e do controlo das fronteiras, na medida em que a sua utilização se permita nos termos do direito da União ou do direito nacional aplicável:

Especificamente, sistemas de IA concebidos para ser empregues por autoridades públicas competentes (ou em seu nome, ou por instituições, órgãos ou organismos da União),

- (i) como polígrafos e instrumentos semelhantes;
- (ii) para avaliação dos riscos, incluindo um risco para a segurança, um risco de migração irregular ou um risco para a saúde, que uma pessoa singular que pretenda entrar ou tenha entrado no território de um Estado-Membro represente;
- (iii) para auxiliar as autoridades públicas competentes na análise de pedidos de asilo, de visto e de autorização de residência e das queixas conexas, no que toca à elegibilidade das pessoas singulares que requerem determinado estatuto, nomeadamente nas avaliações conexas da fiabilidade dos elementos de prova;
- (iv) no contexto da gestão da migração, do asilo ou do controlo das fronteiras, para efeitos de detecção, reconhecimento ou identificação de pessoas singulares, com excepção da verificação de documentos de viagem.

2.8. Administração da justiça e processos democráticos:

Sistemas de IA concebidos para ser empregues

- (i) Por uma autoridade judiciária, ou em seu nome, para auxiliar uma tal autoridade na investigação e na interpretação de factos e do direito, bem como na aplicação da lei a um conjunto específico de factos, ou de forma similar na resolução alternativa de litígios;
- (ii) Para influenciar o resultado de uma eleição ou referendo ou o comportamento eleitoral de pessoas singulares no exercício do seu direito de voto em eleições ou referendos: neles não se incluem os sistemas de IA a cujos resultados as pessoas singulares não estejam directamente expostas, como as ferramentas utilizadas para organizar, otimizar e estruturar campanhas políticas do ponto de vista administrativo e logístico.

3. Breve análise de dados sistemas incluídos nos de risco elevado

Neste particular, contemplemos só – e tão só – os sistemas que se socorrem dos dados biométricos, tendo em vista uma análise breve, perfunctória, dada a extensão dos temas neste passo imbricados.

O Regulamento considera, com efeito, como de risco elevado, os sistemas assentes em dados biométricos cujo emprego se consinta, ao abrigo do direito da União ou do ordenamento pátrio aplicável, com exclusão obviamente dos que figuram no *índice* porque proscritos.

E nesse passo figuram os sistemas:

- de identificação biométrica à distância, com uma exclusão, a saber, a dos sistemas que se concebem com o único propósito de confirmar que uma dada pessoa natural é, de facto, quem alega ser;
- cuja concepção permita aferir a categorização biométrica, de acordo com atributos ou características sensíveis ou protegidos com base na sua inferência;
- cujo modelo permita o reconhecimento de emoções.

A biometria permite que uma pessoa natural seja identificada e autenticada com base em dados reconhecíveis, verificáveis, únicos e específicos.

Autenticação biométrica compara os dados das características da pessoa natural com o "modelo" biométrico de uma tal pessoa para determinar a sua verosimilhança.

O modelo de referência é previamente colectado.

Os dados recopilados são então comparados com os dados biométricos da pessoa alvo ou sujeita a autenticação.

A identificação biométrica consiste, por seu turno, em determinar a identidade de uma pessoa natural (ou física, se se pretender).

O objectivo é o de “capturar” um dado biométrico de uma tal pessoa: pode ser, *v.g.*, uma foto do rosto, uma gravação da voz ou uma imagem da impressão digital.

Estes dados são então comparados com os dados biométricos de várias outras pessoas mantidos numa base de dados.

Daí que se revista de peculiares cautelas para que os sistemas de risco elevado, como no caso, não atentem contra os direitos plasmados na Carta de Direitos Fundamentais da União Europeia.

Esse é o magno objectivo consubstanciado, de resto, no Regulamento a cuja análise parcial se vem de proceder, circunscrita aos restritos temas em debate sobre que se intentou fazer luz.

BIBLIOGRAFIA

AI HLEG - High-Level Expert Group on Artificial Intelligence. A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines. Brussels. 2019. Disponível em <https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

BRADFORD, Anu. The Brussels effect: how the European Union rules the world. New York: Oxford University Press, 2020. Kindle edition.

CDEI – Centre for Data Ethics and Innovation. The European Commission's artificial intelligence act highlights the need for an effective AI assurance ecosystem. 2021. Disponível em: <https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem/>.

CURZON, James; et al. "Privacy and Artificial Intelligence. IEEE Transactions on Artificial Intelligence 2.2, 2021. p. 96-108. Disponível em:

<https://ieeexplore-ieee-org.ez433.periodicos.capes.gov.br/stamp/stamp.jsp?tp=&arnumber=9450036>.

EBERS, Martin. Standardizing AI-The Case of the European Commission's Proposal for an Artificial Intelligence Act. The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics, 2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3900378.

EUROPEAN COMMISSION. Ethics guidelines for trustworthy AI. 2019. Disponível em:

<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

EUROPEAN COMMISSION. Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. Brussels. 2021. Disponível em:

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.

EUROPEAN COMMISSION. White paper on artificial intelligence: a European approach to excellence and trust. Brussels. 2020. Disponível em: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

FLORIDI, Luciano. The European Legislation on AI: A brief analysis of its philosophical approach. Philosophy & Technology, v. 34, n. 2, p. 215-222, 2021. Disponível em: <https://link.springer.com/article/10.1007/s13347-021-00460-9>.

FOTA, Mário. “A disciplina da inteligência artificial in itinere na União Europeia”, in “Revista Judiciária do Paraná, editora Bonijuris, Curitiba, n.º 27, Set-Out-Nov-2023, pp. 136-150

“O marco europeu da Inteligência Artificial e as precauções no domínio dos riscos proscritos”, in “Revista Judiciária do Paraná, editora Bonijuris, Curitiba, n.º 30 (no prelo)

KAAL, Wulf A. Dynamic regulation for innovation. Perspectives in Law, Business & Innovation (Mark Fenwick, Wulf A. Kaal, Toshiyuki Kono & Erik PM Vermeulen eds.). New York Springer (2016), U of St. Thomas (Minnesota) Legal Studies Research Paper n. 16-22, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2831040.

KOP, Mauritz. EU Artificial Intelligence Act: The European Approach to AI. Transatlantic antitrust and IPR Developments, 2021. Disponível em:

<https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/>.

MÖKANDER, Jakob et al. Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, v. 32, n. 2, p. 241-268, 2022. Disponível em: <https://link.springer.com/article/10.1007/s11023-021-09577-4>.

MÖKANDER, Jakob et al. Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, v. 32, n. 2, p. 241-268, 2022. Disponível em: <https://link.springer.com/article/10.1007/s11023-021-09577-4>.

NWAFOR, Ifeoma Elizabeth. AI ethical bias: a case for AI vigilantism (Aillantism) in shaping the regulation of AI. *International Journal of Law and Information Technology*, v. 29, n. 3, p. 225-240, 2021. Disponível em: <https://academic.oup.com/ijlit/article/29/3/225/6389717?login=true>.

REJMANIAK, Rafal. Bias in Artificial Intelligence Systems. *Bialostockie Studia Prawnicze*, v. 26, p. 25, 2021. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/bialspw26&div=36&id=&page=>.

ROSALINO, Helder, O impacto regulatório da IS: uma análise do AI Act no contexto financeiro europeu, in “Espresso”, Lisboa, 12 de abril de 2024, p. 29

SAYEG, Rodrigo, Regulamentação da IA para aproveitar as oportunidades oferecidas pela sociedade de dados: o exemplo da União Europeia, *Diário de São Paulo*, 29 de Abril de 2024, p. 10

SÁNCHEZ BRAVO, Álvaro Avelino. Marco Europeo para una inteligencia artificial basada en las personas. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, p. 65-78, jan./abr. 2020. Disponível em: <https://journal.nuped.com.br/index.php/revista/article/view/sanchezbravov1n1/262>.

TEUBNER, Gunther. Das regulatorische Trilemma: Zur Diskussion um post-instrumentale Rechtsmodelle. *Quaderni Fiorentini per la storia del pensiero giuridico moderno*, v. 13, n. 1, p. 109-149, 1984. Disponível em: <http://www.centropgm.unifi.it/cache/quaderni/13/0112.pdf>.

UFERT, Fabienne. AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI? *European Papers-A Journal on Law and Integration*, v. 2020, n. 2, p. 1087-1097, 2020. Disponível em: <https://www.europeanpapers.eu/it/europeanforum/ai-regulation-through-the-lens-of-fundamental-rights>.