ISSN: 1696-3083, Revista Galega de Dereito Social -2ª ET- (18,2023), pp. 41-74
http://www.revistagalegadedereitosocial.gal

OBRIGAS DO EMPRESARIO EN MATERIA DE PREVENCIÓN DE RISCOS LABORAIS DERIVADAS DA UTILIZACIÓN DE SISTEMAS DE IA*

BEATRIZ RODRÍGUEZ SANZ DE GALDEANO
Profesora titular de Dereito do Traballo e da Seguridade Social
Universidade Pública de Navarra
beatriz.rodriguez@unavarra.es

RESUMO

O obxectivo do presente estudo é analizar cales son as obrigas do empresario que incorpora produtos de traballo ou sistemas de *software* baseados na intelixencia artificial. Para iso, realízase unha caracterización xenérica destes novos desenvolvementos tecnolóxicos e das oportunidades e retos que formulan en materia preventiva. Posteriormente, descéndese á análise de cales son as obrigas do empresario que incorpora estes novos equipos con fins produtivos, de xestión de recursos humanos ou para o cumprimento das súas obrigas preventivas. Para iso, pártese, en primeiro lugar, da normativa xeral de seguridade dos produtos e da normativa específica sobre sistemas de IA; en segundo lugar, analízanse as obrigas derivadas da normativa de protección de datos cando se introducen equipos dotados con sistemas de IA que implican un tratamento de datos; por último, estúdanse as obrigas específicas en materia de prevención de

* Artigo realizado no marco as actividades de investigación correspondentes ao Proxecto de Xeración do Coñecemento "Intelixencia artificial e Prevención de Riscos Laborais: retos para a normativa preventiva e en materia de responsabilidade " (PID2021-123514NB-I00), IP: Prof. Dr. José Luis Goñi Sein. Universidade Pública de Navarra.

Recibido: 02/06/2023; Aceptado: 20/07/2023

riscos laborais, profundando nas súas conexións coa nova normativa sobre IA.
Palabras chave: Intelixencia artificial; seguridade do produto; obrigas preventivas do empresario; responsabilidade civil por produtos defectuosos.

RESUMEN

El objetivo de del presente estudio es analizar cuáles son las obligaciones del empresario que incorpora productos de trabajo o sistemas de software basados en la Inteligencia Artificial. Para ello, se realiza una caracterización genérica de estos nuevos desarrollos tecnológicos y de las oportunidades y retos que plantean en materia preventiva. Posteriormente, se desciende al análisis de cuáles son las obligaciones del empresario que incorpora estos nuevos equipos con fines productivos, de gestión de recursos humanos o para el cumplimiento de sus obligaciones preventivas. Para ello, se parte, en primer lugar, de la normativa general de seguridad de los productos y de la normativa específica sobre sistemas de IA; en segundo lugar, se analizan las obligaciones derivadas de la normativa de protección de datos cuando se introducen equipos dotados con sistemas de IA que implican un tratamiento de datos; por último, se estudian las obligaciones específicas en materia de prevención de riesgos laborales, ahondando en sus conexiones con la nueva normativa sobre IA.
Palabras clave: Inteligencia Artificial; Seguridad del Producto; Obligaciones Preventivas del Empresario; Responsabilidad civil por productos defectuosos.

SUMARIO

DE HARMONIZACIÓN TÉCNICA; 2.2. NORMATIVA DE SEGURIDADE RELATIVA AOS SISTEMAS DE IA: APROXIMACIÓN BASEADA NO RISCO; 2.2.1 Sistemas prohibidos; 2.2.2 Sistemas de alto risco; 2.2.3. Sistemas que non son de alto risco; 2.2.4. Obrigas de transparencia para determinados sistemas de IA; 2.3 CANLES DE COORDINACIÓN EN MATERIA DE AVALIACIÓN ENTRE A PROPOSTA DE LEI DE IA E A NORMATIVA SECTORIAL DE SEGURIDADE DO PRODUTO. **3. AS OBRIGAS DO EMPRESARIO EN CANTO USUARIO DE PRODUTOS BASEADOS EN SISTEMA DE IA DERIVADAS DA NORMATIVA EN MATERIA DE SEGURIDADE DO PRODUTO E DA LEI IA;** 3.1. UTILIZACIÓN CONFORME O USO PREVISTO OU RAZOABLEMENTE PREVISIBLE; 3.2. OBRIGAS ESPECÍFICAS PARA O USUARIO DE SISTEMAS DE IA; 3.3.- O EMPRESARIO COMO FABRICANTE: A ALTERACIÓN DO PRODUTO OU SISTEMA DE IA. **4. AS OBRIGAS DO EMPRESARIO EN MATERIA PREVENTIVA. 5. AS OBRIGAS DO EMPRESARIO EN MATERIA DE PROTECCIÓN DE DATOS. 6. APROXIMACIÓN Á NOVA NORMATIVA EN MATERIA DE RESPONSABILIDADE CIVIL DERIVADA DE PRODUTOS DEFECTUOSOS E POR DANOS CAUSADOS POR SISTEMAS DE IA. 7. BIBLIOGRAFÍA.**

1. INTRODUCIÓN: INCORPORACIÓN DA IA NA EMPRESA E O SEU IMPACTO EN MATERIA DE PREVENCIÓN DE RISCOS LABORAIS

Os desenvolvementos tecnolóxicos baseados en sistemas de intelixencia artificial (en diante IA), están a ser incorporados á organización produtiva da empresa de diversos modos e con diferentes finalidades.

É xa unha realidade a utilización de equipos robóticos avanzados que incorporan sistemas de IA, co fin de mellorar a súa eficacia e asegurar o seu adecuado mantemento e

supervisión[1]. A incorporación aos robots tradicionais de sensores capaces de interactuar coa contorna e de sistemas de tratamento de datos para executar tarefas de forma autónoma, deu lugar a unha nova xeración de robots, que está a liderar en gran medida a nova revolución industrial. Estes equipos poden ser adquiridos polo empresario directamente do fabricante. Trataríase, por tanto, de produtos que incorporan xa solucións baseadas en sistemas de IA. Pero tamén é posible que o empresario adquira directamente sistemas de IA co fin de incorporalos aos seus propios equipos para mellorar ou desenvolver certas utilidades. Nestes casos, o fin primordial do empresario adoita ser incorporalos á súa organización produtiva para mellorar o rendemento.

Así mesmo, os equipos que incorporan sistemas de IA tamén poden ser adquiridos polo empresario co fin de destinalos ao cumprimento de determinadas obrigas preventivas. É o caso, por exemplo, dos drons baseados en sistemas de IA, que se utilizan co fin de supervisar as condicións de seguridade nas que se desenvolven determinadas operacións complexas. Deste xeito, o empresario pode cumprir as obrigas específicas de coordinación e supervisión que lle impón a normativa preventiva.

Tamén comeza a ser frecuente a utilización de *software*, baseado en IA, con fins de xestión de recursos humanos [2]. Trátase de programas informáticos que permiten obter información sobre o desenvolvemento do traballo, rendemento dos equipos etc., co fin xenérico de mellorar a produtividade e eficiencia da empresa. En ocasións este *software* incorpórase aos propios equipos de traballo para ter

[1]EU-OSHA: *Advanced robotics and automation: implications for occupationl safety and health,* 2022, dispoñible en: https://osha.europa.eu/en/publications/advanced-robotics-and-automation-implications-occupational-safety-and-health

[2] EU-OSHA: *Artificial intelligence for worker management: an overview,* 2022, dispoñible en https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-overview

un coñecemento óptimo e en tempo real sobre o funcionamento destes equipos. Estes sistemas baséanse no procesamento de datos, persoais ou non.

Estes sistemas entrañan na maioría das ocasións un control do propio traballador e, dende este punto de vista, pode que as decisións que se adopten consistan na simple formulación de recomendacións sobre a forma correcta de desenvolver o traballo, ou que pretendan a avaliación do traballador e dos seus posibles erros ou mesmo servir como base para a adopción de medidas disciplinarias[3].

Este *sofware* pode ser adquirido directamente polo empresario e, en tal caso, como se verá, haberá de asegurarse de que responde aos requirimentos de seguridade e observar o resto de normativa preventiva e en materia de protección de datos. Aínda que tamén pode ocorrer que o empresario non adquira directamente este *software*, senón que opte por contratar a un terceiro, que utiliza este tipo de sistemas co fin de prestar un servizo relativo, por exemplo, ao control de incapacidades, do estado de saúde dos traballadores etc.

Dende o punto de vista lexislativo estes avances tecnolóxicos requiren adaptacións dun marco normativo que, na súa actual configuración, non ofrece resposta aos principais interrogantes que suscita esta nova revolución. Como en anteriores ocasións, a evolución da técnica sitúase un paso por diante do marco normativo vixente. Xunto a iso, a revolución tecnolóxica actual, a diferenza doutras anteriores, caracterízase pola súa complexidade e pola súa rápida extensión ás máis diversas áreas vitais.

Doutra banda, ha de terse en conta que calquera intervención lexislativa debe ponderar os diversos intereses en xogo. Non cabe dúbida de que resulta necesario asegurar un nivel adecuado de seguridade e prevención dos riscos que estes

[3] EU-OSHA: *Artificial intelligence for worker management: mapping definitions, uses and implications,* 2022, dispoñible en: https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-mapping-definitions-uses-and-implications

novos avances entrañan, sen descoñecer ao mesmo tempo o impacto positivo que poden ter no noso desenvolvemento vital e os importantes intereses económicos en xogo.

Á luz deste panorama brevemente descrito, a cuestión que se propón, deixando á parte os supostos de contratación de servizos con terceiros, é cales son as obrigas que ha de asumir o empresario que incorpora este tipo de produtos baseados en sistemas de IA á súa empresa.

Para abordar esta cuestión é necesario conxugar tres bloques normativos diversos: por unha banda, a normativa de seguridade do produto, incluída a proposta de Regulamento de IA; doutra banda, a normativa en materia de prevención de riscos laborais; e, por último, a normativa en materia de protección de datos. Non se abordan con detemento as posibles responsabilidades polos danos causados por tales produtos, aínda que se dedica un breve apartado final á presentación dos avances normativos que no ámbito da responsabilidade civil están a impulsarse dende Europa.

2. A OBRIGA DE ADQUIRIR PRODUTOS SEGUROS E O IMPACTO DA PROPOSTA DE LEI DE IA

A primeira obriga do empresario que incorpora produtos baseados en sistemas de IA é asegurarse de que eses produtos cumpran coa normativa existente en materia de seguridade. Para iso, o fabricante haberá de ter en conta, en primeiro lugar, as disposicións específicas, se existen, relativas ao concreto produto (máquinas, EPI etc.) e, en segundo lugar, os requisitos de seguridade para sistemas baseados en IA esixidos pola nova Lei de IA.

2.1. NORMATIVA ESPECÍFICA DE SEGURIDADE DO PRODUTO: O NOVO ENFOQUE EN MATERIA DE HARMONIZACIÓN TÉCNICA

A normativa de seguridade do produto ten como obxectivo principal garantir un nivel elevado de seguridade dos produtos que se comercializan na UE e evitar os obstáculos ao libre comercio. Para conseguir este obxectivo a normativa

de seguridade baséase no denominado novo enfoque en materia de harmonización, co que se pretende garantir unha adaptación rápida das esixencias de seguridade[4]. Para iso, as directivas ou regulamentos comunitarios limítanse a recoller os requisitos de seguridade que deben reunir os produtos. O fabricante que pretenda comercializar un produto na UE ha de levar a cabo as avaliacións do produto co fin de acreditar que reúne os requisitos de seguridade. Para facilitar este proceso presúmese a conformidade cos requisitos esenciais de seguridade daqueles produtos que cumpran as normas técnicas, de carácter voluntario, elaboradas polos organismos de normalización. De tal maneira, que a observación destas normas técnicas facilite o proceso de avaliación da conformidade. Os produtos que cumpran os requisitos de seguridade poden incorporar o marcado CE e a declaración CE de conformidade.

No que se refire especificamente aos equipos tradicionalmente destinados a un uso profesional, existe unha normativa consolidada baseada no novo enfoque para produtos tales como: máquinas, equipos de protección individual, equipos a presión etc.

Este sistema tradicional permitiu unha harmonización rápida das esixencias esenciais de seguridade, grazas á efectividade dos organismos de normalización, que realizaron un importante labor de actualización das normas técnicas, sen perder de vista o obxectivo de garantir un elevado nivel de seguridade. No entanto, o desenvolvemento de produtos baseados en sistemas de IA obriga á UE a revisar a súa actuación en materia de seguridade do produto. Con este obxectivo dende a UE se veu traballando na proposta de Regulamento IA, que a continuación se detalla.

[4] Resolución do Consello do 17 de maio de 1985, relativa a unha nova aproximación en materia de harmonización e de normalización.

2.2. NORMATIVA DE SEGURIDADE RELATIVA AOS SISTEMAS DE IA: APROXIMACIÓN BASEADA NO RISCO

Á hora de abordar a regulación dos requisitos de seguridade dos sistemas de IA a UE marcouse un dobre obxectivo: por unha banda, dotar dun marco normativo suficiente para garantir un nivel adecuado de seguridade dos sistemas de IA que se comercializan en Europa; e por outra, coordinar estas novas esixencias coa xa consolidada normativa existente en materia de seguridade do produto.

Con este dobre obxectivo, a UE apostou por unha norma horizontal, a proposta de Regulamento polo que se establecen normas harmonizadas en materia de intelixencia artificial (Lei de intelixencia artificial)[5]. A proposta inicial foi obxecto de multitude de emendas, que foron aprobadas polo Parlamento Europeo o pasado 14 de xuño de 2023[6].

A última proposta, tras as emendas adoptadas, incorpora, no seu art. 4 bis, os principios que han de guiar a actuación de todos os operadores e que son os seguintes: intervención e vixilancia humana, solidez e seguridade técnica, privacidade e gobernanza de datos, transparencia, respecto á diversidade e non discriminación e benestar social e ambiental.

A nova norma opta por definir en termos amplos o seu ámbito de aplicación e ofrecer un marco xeral, baseado na clasificación de riscos. O art. 3.1 define o sistema de IA como: *"un sistema baseado en máquinas deseñado para funcionar con diversos niveis de autonomía e capaz, para obxectivos explícitos ou implícitos, de xerar información de saída —como predicións, recomendacións ou decisións— que inflúa en contornas reais ou virtuais".*

Unha vez definido en termos tan amplos o concepto de sistema de IA, a norma opta por un enfoque baseado no risco, para concretar os requisitos de seguridade esixidos para a posta en circulación destes servizos, en función de se

[5] COM (20221) 106 final, do 21 de abril de 2021.

[6] A última versión, coas emendas aprobadas, pódese consultar en: https://www.europarl.europa.eu/doceo/document/ta-9-2023-0236_É.pdf

se está ante sistemas prohibidos, sistemas de alto risco e o resto de sistemas[7].
Doutra banda, co obxecto de facilitar a coordinación coa normativa xa existente en materia de seguridade, o texto do Regulamento recolle os requisitos esenciais de seguridade que han de reunir determinados sistemas de IA, considerados de alto risco, pero previu que os produtos que xa eran obxecto de normativa específica se sigan rexendo pola dita normativa, aínda que tamén han de respectar os requisitos esenciais de seguridade en materia de IA.
No que se refire á convivencia desta normativa coa específica en materia laboral, o Regulamento no seu art. 2 apartado 5 quater, sinala que a aplicación do disposto no Regulamento, non impide que os Estados introduzan normas máis favorables para os traballadores ou permitan a aplicación de convenios colectivos máis favorables.

2.2.1. Sistemas prohibidos
A proposta de Lei de IA prohibe no seu art. 5 unha serie de sistemas entre os que se inclúen: aqueles baseados no uso das técnicas subliminares, manipuladoras ou enganosas que poidan alterar o comportamento humano; sistemas de IA para a explotación de puntos débiles de grupos de persoas que sexan vulnerables pola súa idade, capacidade, situación social ou económica, cando se causa con tales prácticas un prexuízo significativo; sistemas de categorización biométrica que clasifiquen á persoa conforme atributos ou características sensibles ou protexidas; sistemas que sirvan para a cualificación social de persoas físicas en razón das súas características, personalidade, que conduzan a un trato inxustificado ou desproporcionado de persoas ou grupos, ou a un trato prexudicial; sistemas de identificación biométrica remota en tempo real en espazos de acceso público; sistemas

[7] Goñi Sein, J.L. (2023): Ley de inteligencia artificial y seguridad y salud en el trabajo", en AA.VV. (dir.: Rodríguez Sanz de Galdeano, B. e Egusquiza Balmaseda, M.A.: *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.

de IA para levar a cabo avaliacións de risco de persoas co fin de determinar o risco de que cometan infraccións e os sistemas que cren ou amplíen bases de datos de recoñecemento facial mediante extracción de imaxes faciais a partir de internet ou circuíto pechado de televisión; sistemas para inferir emocións, entre outros ámbitos, no lugar de traballo, e sistemas de identificación biométrica en diferido, salvo que estean suxeitos a unha autorización xudicial e sexan necesarios para a procura selectiva destinada á aplicación da lei e relacionada cun delito grave.
Trátase, como pode observarse, de sistemas que contraveñen os valores da Unión de respecto á dignidade humana, liberdade, igualdade, democracia e Estado de dereito e dos dereitos fundamentais, que recoñece a UE, como o dereito á non discriminación, á protección de datos e á privacidade.

2.2.2. Sistemas de alto risco

Entre os sistemas de alto risco inclúense, en primeiro lugar, aqueles destinados a ser utilizados como compoñente de seguridade dun dos produtos contemplados no Anexo II da proposta e tamén aqueles sistemas que en si mesmos son un destes produtos, sempre que estes produtos conforme a súa propia lexislación de harmonización deban someterse a unha avaliación externa. Entre os produtos que recolle o Anexo atópanse produtos sometidos á normativa do novo enfoque e destinados a ser utilizados no ámbito profesional tales como as máquinas, equipos de protección individual, equipos a presión, aparellos para uso en atmosferas explosivas, ascensores. Agora ben, non abonda con que o sistema de IA se incorpore ou sexa un destes produtos, senón que ademais é necesario que requira avaliación de conformidade dun terceiro. Este tipo de avaliacións de conformidade contémplanse na normativa sectorial de seguridade de cada produto e a súa imposición depende do grao de perigo. Así, por exemplo, no caso das máquinas requírese a dita avaliación por terceiro cando se trate dalgunha das máquinas

incluídas no Anexo IV entre as que figuran serras, plataformas elevadoras, máquinas moldeadoras, máquinas portátiles de impacto etc.

En segundo lugar, considéranse sistemas de alto risco, segundo o art. 6.2 da proposta, os mencionados no Anexo III coa condición, engadida tras o trámite de emendas, de que entrañen un risco significativo de causar prexuízos para a saúde, a seguridade ou os dereitos fundamentais das persoas físicas. O Anexo toma como criterio o uso e o ámbito ao que se destina o sistema de IA. No que aquí interesa, inclúense sistemas destinados a ser utilizados para extraer conclusións sobre as características físicas das persoas a partir de datos biométricos; sistemas dirixidos a avaliar o nivel de educación dunha persoa e influír no nivel de educación e formación que vai recibir; sistemas para a contratación e a selección de traballadores e os sistemas destinados a adoptar decisións en materia de promoción ou asignación de tarefas, avaliación do rendemento e conduta dos traballadores no marco das ditas relacións; sistemas de IA destinados a ser utilizados nos seus sistemas de recomendación por plataformas de redes sociais, designadas como plataformas en liña de moi gran tamaño. Ha de terse en conta que, tras o trámite de emendas, introduciuse no art. 6 un apartado 2 bis, en virtude do cal se permite aos provedores presentar unha notificación motivada á autoridade nacional de supervisión cando consideren que o seu sistema de IA non presenta un risco significativo.
A proposta de Lei de IA obriga o fabricante destes sistemas de alto risco a implantar, documentar e manter un sistema de xestión de riscos que inclúe: a identificación, a estimación e a avaliación dos riscos coñecidos e razoablemente previsibles para a seguridade e a saúde, para os dereitos fundamentais, incluída a igualdade de acceso e de oportunidades, a democracia ou o medio ambiente, cando se utilice conforme á finalidade prevista ou en condicións de uso indebido razoablemente previsibles; a avaliación dos riscos significativos emerxentes; a adopción das medidas oportunas

de xestión de riscos. (art. 9). Ademais, no caso de que os sistemas de IA utilicen técnicas que implican o adestramento con modelos de datos, haberán de cumprirse os criterios de calidade previstos nos apartados 2 a 5 do art. 10 da proposta, entre os que se inclúe un exame que atenda á existencia de nesgos que poidan dar lugar a discriminacións prohibidas.
O proceso complétase coa previsión dun sistema de avaliación da conformidade (art. 43), dirixido a demostrar o cumprimento dos requisitos de seguridade esixidos polo Regulamento. Cando se supere esta avaliación de conformidade, os sistemas de IA incorporarán o marcado CE de conformidade. Engádese, ademais, que os sistemas de IA de alto risco que sexan conformes con normas harmonizadas entenderanse conformes cos requisitos esenciais de seguridade. Obsérvase como o esquema trazado para garantir a seguridade destes sistemas de alto risco baséase na filosofía inspiradora do novo enfoque en materia de harmonización. Ocorre, con todo, que na actualidade non existe unha referencia de especificacións técnicas en materia de IA, similar á existente para outros produtos como máquinas ou EPI. Por iso, como novidade, a proposta de IA contempla a posibilidade de que a Comisión elabore especificacións comúns, que recollan estándares técnicos. Estas especificacións aprobaranse para o caso de que non haxa normas harmonizadas ou cando sexan insuficientes. Para a súa elaboración a Comisión ha de solicitar os puntos de vista dos organismos e grupos de expertos pertinentes.

2.2.3. Sistemas que non son de alto risco

Os provedores de sistemas que non sexan considerados de alto risco segundo a proposta de lei de IA, poderán voluntariamente cumprir os requisitos de seguridade impostos aos sistemas de alto risco. Co obxecto de promover esta aplicación voluntaria, establécese que a Comisión e o Comité promoverán a elaboración de códigos de conduta tendentes a facilitar o cumprimento dos requisitos de seguridade (art. 69).

Ábrese, por tanto, un espazo non regulado, que en boa medida dependerá do desenvolvemento deses códigos de conduta e da súa utilidade para o desenvolvemento de sistemas de IA que non son de alto risco.

2.2.4. Obrigas de transparencia para determinados sistemas de IA

O art. 52 da proposta contempla obrigas para os sistemas de IA, sexan ou non de alto risco, destinados a interactuar con persoas físicas. Nestes casos deberase informar polo sistema de IA ou polo propio provedor ou usuario ás persoas expostas de que están a interactuar cun sistema de IA, salvo cando resulte evidente. Ademais, informarase cando proceda das funcións habilitadas pola IA, de se existe vixilancia humana e de quen é o responsable da toma de decisións.

2.3. CANLES DE COORDINACIÓN EN MATERIA DE AVALIACIÓN ENTRE A PROPOSTA DE LEI DE IA E A NORMATIVA SECTORIAL DE SEGURIDADE DO PRODUTO

Tal e como se viu, os sistemas de IA poden integrarse en equipos xa existentes, por exemplo, unha máquina ou un EPI, co fin de mellorar a súa eficacia ou introducir novas utilidades. Nestes casos, suscítase a necesidade de coordinar as esixencias de seguridade específicas, contempladas na normativa sectorial de cada produto e as esixencias de seguridade propias dos sistemas de IA de alto risco.

Para iso, a proposta de lei de IA previu que en tales casos os equipos se sometan á avaliación de conformidade, de acordo coa normativa sectorial específica, e que, no marco dese proceso de avaliación da conformidade, se comprobe tamén o cumprimento dos requisitos obrigatorios relativos aos sistemas de IA de alto risco. De tal maneira que o marcado CE acreditará o cumprimento dos requisitos de seguridade do concreto produto e tamén do sistema de IA.

3. AS OBRIGAS DO EMPRESARIO EN CANTO USUARIO DE PRODUTOS BASEADOS EN SISTEMAS DE IA DERIVADAS DA NORMATIVA EN MATERIA DE SEGURIDADE DO PRODUTO E DA LEI IA

A normativa que establece os requisitos de seguridade dos produtos ten como principal destinatario o provedor deses produtos. Tal e como se viu, o fabricante será quen deba observar os requisitos obrigatorios de seguridade e acreditar o seu cumprimento mediante a correspondente avaliación de conformidade. De tal maneira que a principal obriga do empresario será asegurarse de que os produtos que adquire son seguros.

Agora ben, máis aló deste momento inicial de adquisición do produto, durante a súa utilización o empresario, en canto usuario del, ha de observar unha serie de obrigas que derivan directamente da normativa de seguridade do produto e que, no caso de utilización de sistemas de IA, presentan especialidades derivadas das particularidades deste tipo de sistemas, motivadas fundamentalmente porque o seu comportamento pode verse alterado con posterioridade á comercialización.

3.1. UTILIZACIÓN CONFORME O USO PREVISTO OU RAZOABLEMENTE PREVISIBLE

Con carácter xeral, o empresario está obrigado a utilizar os equipos para os fins para os que foron deseñados e así o contempla expresamente o art. 41 LPRL. Dende un punto de vista concreto, na definición de seguridade contida na Directiva sobre seguridade xeral dos produtos e na proposta de Regulamento xeral, o concepto de produto seguro relaciónase cos seus usos razoables[8]. De tal maneira, que o fabricante ha de garantir un nivel elevado de seguridade en

[8] Directiva 2001/95, do 3 de decembro. Está a ser obxecto de revisión e na actualidade existe xa unha Proposta, do 30 de xuño de 2021, do Parlamento Europeo e do Consello, relativa á seguridade xeral dos produtos, COM 2021/346 final.

tales condicións. En contrapartida, o empresario debe utilizar os produtos para os fins para os que foron deseñados e que razoablemente cabe esperar. Na normativa específica sectorial, reitéranse estas referencias ao uso previsto en condicións razoables.

No que se refire en particular aos sistemas de IA, o art. 3 da proposta de lei IA, tras as emendas do Parlamento, preferiu optar pola denominación de implementador, en lugar de usuario, para referirse á persoa física ou xurídica, autoridade pública, axencia ou organismo doutra índole que utilice un sistema de IA baixo a súa propia autoridade, salvo cando o seu uso se enmarque nunha actividade persoal de carácter non profesional. De acordo con esta definición, o empresario que utiliza o sistema de IA como medio de produción na súa empresa, tería a condición de implementador a efectos da IA. Este rol do empresario engade novas obrigas ás tradicionalmente recollidas pola normativa de seguridade do produto e prevención de riscos laborais.

As obrigas que a proposta impón aos implementadores refírense aos casos de utilización de sistemas cualificados como de alto risco. Estes sistemas, tal e como se viu anteriormente, son aqueles sistemas de IA que son un produto sometido a lexislación de harmonización ou un compoñente de seguridade deses produtos e que, conforme a súa normativa específica, a avaliación de conformidade precisa a intervención dun organismo independente. Así mesmo, han de considerarse de alto risco o sistemas de IA utilizados no ámbito do emprego para algunha das finalidades recollidas no apartado 4 do Anexo III.

Con carácter xeral e profundando na obriga de utilizar os produtos conforme a súa finalidade, a proposta de lei de IA introduce unha serie de obrigas que incumben fundamentalmente ao provedor, co fin de asegurar que o usuario, o empresario neste caso, realiza un uso adecuado dos sistemas. Así, o art. 9.4 c) inclúe entre as medidas de xestión de riscos a información sobre os riscos derivados dun uso adecuado e dun uso indebido razoablemente previsible.

Para estes efectos, sinálase que se terá en conta a experiencia, educación e formación do usuario e que, cando proceda, pode resultar necesario impartir formación aos usuarios. O art. 13 refírese especificamente ao modo en que debe trasladarse a información aos usuarios e sinala que se ha de garantir que os sistemas funcionen cun nivel de transparencia suficiente para que aqueles interpreten e usen correctamente a información de saída. Ademais, sinala que deberán ir acompañados das instrucións de uso adecuadas, que deben incluír información concisa, completa, correcta e clara, de maneira pertinente, accesible e comprensible. En concreto, sinala que esta información debe especificar a finalidade prevista, calquera circunstancia asociada á súa utilización prevista ou uso indebido razoable que poida dar lugar a un risco, o seu funcionamento en relación con persoas que poidan utilizar tales sistemas, a vida útil do sistema, as medidas de vixilancia humana que deben adoptarse e as medidas de mantemento e coidado, incluíndo o referido á actualización do *software*.

3.2. OBRIGAS ESPECÍFICAS PARA O IMPLEMENTADOR DE SISTEMAS DE IA

Á marxe destas obrigas destinadas fundamentalmente a garantir un uso adecuado do sistema de IA, conforme o seu deseño, a proposta de lei de IA, introduce obrigas novas, derivadas das peculiaridades propias dos sistemas de IA, que non tiveron precedente na normativa sectorial específica de seguridade do produto.

Así, o art. 14 obriga a arbitrar medidas de vixilancia humana respecto dos sistemas de alto risco durante o seu tempo de funcionamento. O obxectivo desta vixilancia é reducir ao mínimo posibles riscos para a saúde, seguridade ou dereitos fundamentais. No caso de utilización destes sistemas no ámbito laboral, será o empresario o encargado de garantir estas medidas de vixilancia humana de acordo coa información que lle facilitara o provedor e que debe especificarse na documentación técnica.

Así mesmo, o empresario, como usuario dun sistema de alto risco, ha de observar as obrigas recollidas no art. 29 da proposta de Lei de IA, entre as que se inclúen: asegurarse de que os datos de entrada son pertinentes para a finalidade prevista do sistema de IA; aplicar as medidas de supervisión humana necesarias, vixiar o funcionamento do sistema e informar de posibles incidentes; interromper se fose necesario o seu funcionamento e informar as autoridades en caso necesario; conservar os arquivos de rexistro que se xeran automaticamente e utilizar a información facilitada para cumprir a obriga de avaliación de impacto relativa á protección de datos. Ademais, os usuarios de sistemas de IA de alto risco deberán conservar os arquivos de rexistro que tales sistemas xeren, na medida en que estean baixo o seu control.

Doutra banda, o art. 61 da proposta de lei de IA introduce obrigas de seguimento posterior á comercialización que incumben fundamentalmente aos provedores, pero que tamén poden implicar os usuarios. En xeral, obrígase aos provedores a establecer e documentar un sistema de seguimento posterior á comercialización e sinálase que ese sistema solicitará datos pertinentes sobre o funcionamento dos sistemas de IA. Estes datos poden ser proporcionados polos usuarios, no noso caso o empresario, ou mediante outras fontes.

Por último, o art. 52 da proposta de lei de IA obriga os usuarios de sistemas de IA que xeren ou manipulen contido de imaxe, son ou vídeo que se asemelle notablemente a persoas, obxectos, lugares ou outras entidades ou sucesos existentes e que poidan inducir a considerar que son reais, a facer público que o contido foi xerado de forma artificial. Esta situación podería xerarse cando se utilicen simulacións no ámbito preventivo, con fins de información, formación ou adestramento. Este mesmo artigo, segundo se viu, obriga tamén os usuarios de sistemas de IA destinados a interactuar con persoas físicas a informar as persoas expostas de que están a interactuar con sistemas de IA.

3.3. O EMPRESARIO COMO FABRICANTE: A ALTERACIÓN DO PRODUTO OU SISTEMA DE IA

Con carácter xeral as obrigas sobre os requisitos de seguridade dos produtos teñen como destinatario principal ao fabricante, provedor ou importador que comercializa o produto na UE. Con todo, pode haber ocasións nas que o produto, unha vez comercializado, sufra alteracións. Neste caso a normativa de seguridade do produto, cando esas alteracións sexan substanciais, considera que se está ante un novo produto e que a persoa que introduciu tales alteracións debe ser considerada fabricante e, en consecuencia, ha de someter novamente o produto ao cumprimento dos requisitos esenciais de seguridade.

Así a Guía azul sobre aplicación das normas de produto, sinala que: "Un produto que foi obxecto de cambios ou de revisións para modificar as súas prestacións, os seus fins ou o seu tipo orixinais pode ser considerado un produto novo. A persoa que leva a cabo os cambios converterase no fabricante e deberá asumir as obrigas correspondentes.

As actualizacións de *software* ou as reparacións poden ser incluídas entre as operacións de mantemento sempre que non modifiquen un produto xa introducido no mercado de tal maneira que poidan afectar á súa observancia dos requisitos vixentes".[9]

Na mesma liña, a proposta de Regulamento relativo á seguridade xeral dos produtos[10] sinala no seu art. 12.1 que: "Considerarase fabricante a efectos do presente Regulamento as persoas físicas ou xurídicas, distintas do fabricante, que modifiquen substancialmente o produto; e estarán suxeitas ás obrigas que impón ao fabricante o artigo 8 no que respecta á parte do produto afectada pola modificación ou á totalidade do produto se a modificación substancial repercute na súa seguridade. 2. Considerarase que unha modificación é substancial cando se cumpran os tres criterios seguintes:

[9] Guía azul sobre a aplicación das normas de produto da UE, 2014, páx. 18.
[10] COM (2021) 346 final, do 30 de xuño de 2021.

a) a modificación altera as funcións, o tipo ou o rendemento previstos do produto dunha maneira que non estaba contemplada na avaliación inicial do risco do produto;
b) a natureza do perigo cambiou ou o nivel de risco aumentou debido á modificación;
c) os cambios non foron realizados polo consumidor para o seu propio uso".

No que se refire á normativa específica, directamente relativa a equipos de traballo, ha de destacarse que tamén a proposta de Regulamento de máquinas ten como obxectivo expreso aclarar o concepto de modificación substancial, que xa se recollía na Directiva actualmente vixente[11]. Así, o art. 15 da proposta, titulado: "outros casos en que son aplicables as obrigas dos fabricantes" sinala expresamente que: "Para os efectos do presente Regulamento, considerarase fabricante unha persoa física ou xurídica, distinta do fabricante, o importador ou o distribuidor, que leve a cabo unha modificación substancial da máquina, a parte ou o accesorio, e que, por conseguinte, estará suxeita ás obrigas do fabricante establecidas no artigo 10 con respecto á peza do produto afectada pola modificación ou, se a modificación substancial afecta á seguridade do produto no seu conxunto, con respecto a todo o produto".

Pola súa banda, o art. 3, no seu apartado 16 define modificación substancial como: "unha modificación dunha máquina, unha parte ou un accesorio, por medios físicos ou dixitais, despois de que o dito produto se introduciu no mercado ou foi posto en servizo, que non fose prevista polo fabricante e debido á cal poida verse afectada a conformidade do produto cos requisitos esenciais de saúde e seguridade".

No caso dos sistemas de IA, tamén a proposta de lei de IA contemplou expresamente esta posibilidade e incluíu unha definición de que debe entenderse modificación substancial, no seu art. 3.23, que a define como: "unha modificación ou

[11] Proposta de Regulamento do Parlamento Europeo e do Consello relativa ás máquinas e os seus partes e accesorios COM (2021) 202, final.

serie de modificacións nun sistema de IA tras a súa introdución no mercado ou posta en servizo que non fose prevista ou proxectada polo provedor na avaliación de riscos inicial e como consecuencia da cal resulte afectado o cumprimento por parte do sistema de IA dos requisitos establecidos no título III, capítulo 2, do presente Regulamento ou se modifique a finalidade prevista para a que se avaliou o sistema de IA en cuestión".

De acordo co anterior, o empresario pode erixirse en fabricante e, por tanto, estar obrigado a verificar a conformidade do produto cando introduza cambios substanciais no equipo. A cuestión transcendental é como concretar o significado de modificación substancial e diferencialo doutras modificacións que non entrañan tal carácter substancial e que poden considerarse meras actualizacións. Parece que o elemento determinante se atopa en que a alteración non fose prevista polo fabricante e poida afectar os requisitos esenciais de seguridade. En coherencia co anterior, parece que as actualizacións do equipo previstas polo fabricante non han de considerarse modificacións substanciais porque, en principio, xa foron tidas en consideración na avaliación inicial. Por iso, cando o empresario se limite por exemplo a actualizar o *software* conforme as indicacións do propio fabricante, non estariamos ante un suposto de modificación substancial. Distinto sería o caso cando o empresario actualiza unha máquina, modificando o seu funcionamento, sen o acordo do fabricante ou para un uso non previsto. É nestes casos cando o empresario se equipararía ao fabricante e tería, por tanto, que garantir e acreditar o cumprimento dos requisitos de seguridade e estampar un novo marcado CE.

4. AS OBRIGAS DO EMPRESARIO EN MATERIA PREVENTIVA

A normativa de seguridade do produto, aínda que ten como fin garantir uns estándares elevados de seguridade, non sempre ten en conta as peculiaridades derivadas da

utilización nun ámbito profesional dos equipos. A integración no medio laboral dos produtos entraña riscos específicos que poden ter a súa orixe na propia contorna laboral e nos seus condicionantes físicos e ambientais, na organización do traballo (ritmos de produción, repartición de tarefas) ou nas propias características dos traballadores. A normativa de seguridade e saúde no traballo erixe ao empresario no principal obrigado fronte ao traballador, ao que recoñece o dereito a unha protección eficaz. Co fin de axudar ao empresario no cumprimento de tan esixente obriga, a LPRL vai detallando unha serie de obrigas concretas, algunhas da cales son desenvolvidas en normativa específica. No que se refire aos riscos derivados da utilización de equipos de traballo, ha de estarse ao disposto no art. 41 LPRL, que obriga o empresario a utilizar os equipos conforme os fins recomendados polo fabricante, a instalalos e mantelos de forma adecuada e a informar e formar os traballadores sobre a súa utilización e posibles riscos. De forma específica esta obriga xeral desenvólvese no RD 1215/1992, do 18 de xullo, sobre utilización polos traballadores dos equipos de traballo, o RD 486/97, do 14 de abril, sobre lugares de traballo, ou o RD 485/1997, do 14 de abril, sobre sinalización de seguridade e saúde no traballo.

Así mesmo, o empresario ha de realizar a oportuna avaliación de riscos laborais, de acordo co disposto no art. 16 LPRL e nos art. 3 e seguintes do RD 39/1997, do 17 de xaneiro, que aproba o Regulamento dos servizos de prevención. Nesta avaliación deben tomarse en consideración todos os riscos derivados da elección de equipos de traballo. A avaliación, ademais, ha de manterse actualizada e revisarse cando se detectaron danos ou se aprecie que as actividades de prevención son insuficientes. Esta avaliación de riscos ha de realizarse respecto de todos os equipos e produtos utilizados no traballo e que poidan entrañar algún risco, o cal significa, que a integración de sistemas de IA na empresa, sexan ou non de alto risco, require a previa avaliación de riscos.

A esixencia con que a normativa de prevención de riscos laborais configura a obriga de seguridade do empresario e o amplo elenco de obrigas específicas determina que, na práctica, o empresario se converta no principal obrigado fronte ao traballador e iso a pesar de que tamén a normativa de prevención de riscos impón ao fabricante certas obrigas. Xunto a iso, existen tamén motivos de orde procesual, tales como a facilidade para establecer demanda fronte ao empresario e a inversión da carga da proba, que explican que o empresario sexa o principal obxectivo das reclamacións por danos derivados de accidente.

Non obstante, a complexidade destes novos avances tecnolóxicos e a posibilidade de que existan riscos descoñecidos de cuxo alcance se teña coñecemento despois da comercialización, aconsellarían unha revisión da separación entre as obrigas empresariais e as do fabricante. Doutra banda, ha de terse en conta que o enfoque do Regulamento de IA, baseado nun sistema de pirámide de riscos, só impón o cumprimento de requisitos de seguridade aos sistemas de IA que sexan considerados de alto risco. Ademais, tal e como se viu, a consideración como sistema de IA de alto risco, esixe estar incluído nalgún dos usos especificados polo Anexo e que, ademais, o sistema entrañe un risco significativo. Esta opción do lexislador, pode dar lugar a que existan sistemas que non son de alto risco que se utilicen no ámbito do traballo e que, con todo, poidan entrañar riscos para a seguridade e a saúde ou poidan, mesmo, atentar a dereitos fundamentais.

Noutra orde de consideracións, apuntábase ao comezo que o empresario pode recorrer a estes sistemas de IA con fins produtivos, pero tamén para cumprir parte das súas obrigas preventivas. Sería o caso, por exemplo, de utilización de drons con sistemas de IA para coordinar determinadas actividades perigosas, para apoiar o labor dos recursos preventivos ou coordinadores de seguridade. Igualmente, pode ocorrer que o empresario requira o *software* baseado en IA para realizar determinadas verificacións sobre o estado

de saúde dos traballadores. Non cabe dúbida de que a IA pode apoiar o empresario no cumprimento deste tipo de obrigas. Non obstante, á hora de valorar a súa viabilidade ha de realizarse unha análise detida da LPRL e da súa normativa de desenvolvemento. Así, por exemplo, no referido á coordinación de actividades ou á presenza do recurso preventivo, a LPRL é debedora dun modelo baseado na presenza física da persoa que, por tanto, non poderá ser substituído pola utilización doutras solucións tecnolóxicas, a pesar da súa indubidable utilidade. No que se refire á vixilancia da saúde, haberá de estarse ás posibilidades que para a realización de recoñecementos recolle o art. 22 LPRL e ás limitacións propias do tratamento de datos, que han de categorizarse como sensibles.

5. AS OBRIGAS DO EMPRESARIO EN MATERIA DE PROTECCIÓN DE DATOS

Unha das novidades principais da incorporación destes novos desenvolvementos tecnolóxicos con diferentes fins na empresa é que en moitos casos traen consigo o tratamento de datos do traballador. Esta circunstancia fai necesario revisar o marco xenérico de obrigas que para o empresario se derivan do Regulamento (UE) 2016/679, de Parlamento Europeo e do Consello, en materia de protección de datos (en diante RXPD) e as súas conexións coa proposta de lei de IA.

A propia proposta de lei de IA na súa xustificación sinala que debe aplicarse sen prexuízo do RXPD e nos considerandos sinala que, á hora de valorar o perigo dun sistema de IA, han de terse en conta as súas consecuencias adversas para dereitos fundamentais como o da protección de datos.

Estas declaracións contrastan coa escaseza de preceptos na lei de IA referidos expresamente ás implicacións en materia de protección de datos dos sistemas de IA e que traten de coordinar ambos os bloques. Só o art. 29.6 da proposta contén unha referencia ao RXPD, cando obriga os usuarios dos sistemas de IA de alto risco a utilizar a información fornecida polo fabricante do sistema para levar a cabo a

avaliación de impacto esixida polo art. 35 RXPD. Pola súa banda, o art. 10 da proposta, titulado datos e gobernanza de datos, sinala que os sistemas de alto risco que utilicen técnicas que implican o tratamento de datos, deben desenvolverse a partir de datos que respecten prácticas adecuadas en materia de gobernanza e xestión de datos referidas en particular á elección dun deseño adecuado, a recompilación de datos, as operacións de tratamento para a preparación e datos, a formulación dos supostos, a avaliación previa sobre a dispoñibilidade da cantidade e adecuación de datos necesarios, o exame de posibles sesgos, a detección de lagoas ou deficiencias. Sinala, ademais, que os conxuntos de datos de adestramento, validación e proba serán pertinentes e representativos. Así mesmo, cando sexa necesario, os sistemas de alto risco poderán tratar categorías especiais de datos, coas salvagardas necesarias para o respecto dos dereitos e liberdades fundamentais, entre as cales inclúe a posibilidade de establecer limitacións técnicas á reutilización de datos, tales como a seudonimización ou o cifrado

Cabe apreciar unha sorte de fragmentación entre, por unha banda, as obrigas dos fabricantes de sistemas de IA, centradas en garantir a seguridade e, por outra, as obrigas en materia de protección de datos que parecen incumbir unicamente ao usuario final.

Esta ríxida separación entre a normativa de protección de datos e a de IA determina que, cando o sistema de IA comporte o tratamento de datos, o empresario, como usuario do sistema, adquira a condición de responsable do tratamento de datos e sexa o principal obrigado pola normativa de protección de datos. Estas obrigas variarán segundo as utilidades do sistema de IA, o tipo de datos que se traten e a finalidade que se persiga.

Con carácter xeral, ha de lembrarse que o RXPD se aplica exclusivamente cando exista tratamento de datos persoais, pero non cando os datos que se manexen non teñan tal entidade. Por conseguinte, Haberá supostos nos que os sistemas de IA incorporados polo empresario non recompilen

datos persoais, senón, por exemplo, datos sobre funcionamento e rendemento da maquinaria, sobre a calidade do proceso de produción ou dos propios produtos etc. Haberá, con todo, outros casos nos que si exista o citado tratamento, o cal obriga a respectar os principios e obrigas específicas requiridas polo RXPD.

Nunha aproximación moi xenérica, cabe lembrar que o RXPD pivota sobre os principios de licitude, lealdade e transparencia, que determinan a necesidade de xustificar o tratamento de datos por algunha das bases xurídicas previstas no art. 6 RXPD e de garantir a súa utilización para tal fin

En xeral, no ámbito laboral, poderá xustificarse a necesidade do tratamento por motivos relacionados coa execución do contrato ou co cumprimento dunha obriga legal ou na existencia dun interese lexítimo do interesado. Tal e como se sinalou, os sistemas de IA poden permitir ao empresario o acceso a un amplo volume de información sobre a forma en que se desenvolve a prestación de traballo e sobre os propios traballadores, que poden achar xustificación en motivos tales como a necesidade de supervisar e controlar a actividade laboral, necesidades de organización e dirección ou no cumprimento de obrigas específicas en materia de prevención. Será necesario analizar en cada caso se concorre a base lexítima para o tratamento[12]. Unha vez acreditada a necesidade do tratamento, o empresario debe asegurar o cumprimento do resto de principios en materia de protección de datos que lle esixen garantir os dereitos do interesado, entre os cales están os de información, rectificación, supresión, limitación do tratamento e oposición.

Para asegurar o cumprimento destes principios xerais, o RXPD relaciona nos seus artigos 24 e seguintes toda unha

[12] Véxase.: Baz Rodríguez (2019), J.: *Privacidad y protección de datos de los trabajadores en el entorno digital,* Wolters Kluwer; Goñi Sein, J.L. (2018): *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018),* Bomarzo.

serie de obrigas que han de ser observadas polo responsable do tratamento, no noso caso o empresario. Así se obriga a adoptar as medidas técnicas e organizativas apropiadas para garantir que o tratamento é conforme co RXPD. En concreto obrígaselle a adoptar medidas dende o deseño, entre as que figuran a seudonimización, a minimización. Así mesmo, sinálase que entre as medidas técnicas e organizativas figura o seguimento de políticas de protección de datos e a adhesión a códigos de conduta ou mecanismo de certificación.

O RXPD esixe, por último, a realización dunha avaliación de impacto, cando, con carácter xeral, o tratamento implique un alto risco para os dereitos e liberdades das persoas físicas e, en particular, cando supoña unha avaliación sistemática de aspectos persoais que se base en tratamento automatizado ou na elaboración de perfís sobre cuxa base se tomen decisións con efectos xurídicos. A Axencia Española de Protección de Datos, como autoridade de control, elaborou unha lista indicativa de tratamentos de datos que esixirían tal avaliación, na que figuran os tratamentos que impliquen perfilado ou valoración de suxeitos en ámbitos da súa vida como o desempeño no traballo, tratamentos que impliquen toma de decisións automatizadas, tratamentos que implique a observación, monitorización, supervisión, xeolocalización[13]. Obsérvase, por tanto, como o empresario se erixe no máximo garante do cumprimento dos principios de protección de datos. Existen, con todo, tal e como se sinalaba, momentos nos que quizais non sexa o empresario quen se atope en mellor posición para asegurar o cumprimento de tales principios. Así, por exemplo, o fabricante do sistema IA pode atoparse nunha situación máis adecuada para garantir o tratamento dos datos para as estritas funcionalidades do sistema de IA, garantindo cando fose posible a anonimización. Igualmente, o propio fabricante podería estar en mellor posición para arbitrar dende o mesmo deseño

[13] https://www.aepd.es/es/documento/listas-dpia-é-35-4.pdf

mecanismos que permitisen un fácil exercicio de dereitos como os de acceso e rectificación.

Igualmente, haberá ocasións, nas que o fabricante do sistema IA pode axudar ao empresario ao cumprimento das súas obrigas e, en consecuencia, sería desexable a imposición de certas obrigas específicas, principalmente de información, ao citado fabricante. Así, o deseñador do sistema IA pode axudar ao empresario no cumprimento do deber de transparencia, facilitando nunha linguaxe sinxela información sobre os datos que se recollen, o modo de recollida, o tratamento e a súa finalidade. Tamén o fabricante podería fornecer información valiosa sobre o funcionamento do sistema de IA e as súas posibles aplicacións, co fin de determinar se se está ante un sistema que encaixe nalgún dos supostos de tratamento de datos que require avaliación de impacto.

Así foi posto de manifesto explicitamente no seu informe sobre a proposta pola Axencia Europea de Protección de Datos e polo supervisor europeo de protección de datos. En liña co sinalado neste informe existen diferentes ámbitos e momentos concretos dentro do proceso de fabricación e utilización de sistemas de IA nos que tanto a normativa de IA, como a de protección de datos deberían interactuar de forma explícita.

Non se tratou na proposta de integrar xa no deseño e fabricación dos sistemas de IA os principios que presiden a normativa en materia de protección de datos. Sería interesante, por exemplo, que na proposta de lei se impuxesen ao fabricante de sistemas de IA obrigas co fin de que dende o deseño se evitase o tratamento de datos innecesarios, se incorporaran ao sistema mecanismos que permitisen o exercicio de dereitos como o de cancelación ou corrección.

Así mesmo, tamén debera ser factible que o fabricante realizase unha avaliación de riscos do sistema tendo en conta os posibles usos aos que se destine, o cal á súa vez podería

axudar ao usuario final na súa propia avaliación[14]. En efecto, tanto a proposta de lei de IA como a normativa en materia de protección de datos previron os seus propios mecanismos de avaliación e acreditación da conformidade. Así, tal e como se viu, a proposta de lei de IA, esixe que os produtos de alto risco se sometan a unha avaliación por terceiro. Pola súa banda, o RXPD esixe tamén en determinadas ocasións unha avaliación de impacto. Tendo en conta este marco normativo sería oportuno prever un procedemento de avaliación que servise para ambos os propósitos. Con todo, non foi así, o marcado CE previsto na proposta de lei de IA servirá para acreditar a conformidade con tal proposta, pero non exime da posible realización da avaliación de impacto adicional no caso de que se dean os requisitos previstos no RXPD.

6. APROXIMACIÓN Á NOVA NORMATIVA EN MATERIA DE RESPONSABILIDADE CIVIL DERIVADA DE PRODUTOS DEFECTUOSOS E POR DANOS CAUSADOS POR SISTEMAS DE IA

Cando o traballador sufra un dano como consecuencia da utilización dun produto que incorpora un sistema de IA ou dun sistema de IA autónomo, poderá reclamar a indemnización correspondente, destinada ao resarcimento de tales danos.

A esixencia con que a LPRL, no seu art. 14, configura a obriga de seguridade do empresario, determina que en boa parte dos supostos o empresario asuma a responsabilidade civil derivada de danos causados ao traballador. Xunto a iso, existe a posibilidade de que tamén deba facer fronte a unha eventual responsabilidade administrativa ou penal e á recarga de prestacións.

[14] Así o puxeron de manifesto o EDPD-EDPS no seu comunicado conxunto. EDPB-EDPS. Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 18 de xuño de 2021, dispoñible en https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf

Con todo, ha de terse en conta que no ámbito específico da responsabilidade civil por produtos defectuosos existe un réxime particular, harmonizado a nivel europeo, que está a ser obxecto de revisión. Así mesmo, está a avanzarse nunha norma específica para reparar os danos causados por sistemas de IA[15].

No que se refire á normativa de responsabilidade por produtos defectuosos, aprobouse o pasado 28 de setembro de 2022 a proposta de Directiva do Parlamento Europeo e do Consello sobre responsabilidade polos danos causados por produtos defectuosos[16]. De forma simultánea, o mesmo día viu a luz a Proposta de Directiva de Parlamento Europeo e do Consello, relativa á adaptación das normas de responsabilidade civil extracontractual á intelixencia artificial (Directiva sobre responsabilidade en materia de IA)[17].

Con carácter xeral, a Directiva sobre responsabilidade por produtos defectuosos, que en caso de aprobación derrogará a actual Directiva 85/374, trata de acomodar esta normativa vixente para dar resposta a algúns dos problemas que suscitan a aparición como produtos destes sistemas de IA. Para iso, procede, en primeiro lugar, a adaptar a definición de produto aos novos desenvolvementos derivados da IA. Así, o art. 4.1 da proposta define como produto: "calquera ben moble, aínda cando estea incorporado a outro ben moble ou a un ben inmoble; por produto enténdese tamén (…) os arquivos de fabricación dixital e os programas informáticos". Inclúese, por tanto, expresamente como produto os programas informáticos.

---

[15] EGUSQUIZA BALMASEDA, M.A.: "Marco normativo general y propuestas de regulación en la responsabilidad civil" en AA.VV. (EGUSQUIZA BALMASEDA, M.A. e RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* op. cit. V. tamén na mesma obra: JORQUI AZOFRA, M.: "El concepto legal de producto a la luz de la nueva propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos".

[16] COM 2022/0302

[17] COM 2022 (496) final

O apartado 3 do mesmo artigo define como compoñente: "calquera artigo, tanxible ou intanxible ou calquera servizo conexo que está integrado nun produto ou interconectado con el polo fabricante dese produto ou que estea baixo o seu control". Por último, o servizo conexo é definido no apartado 4 como: "un servizo dixital que está integrado nun produto ou interconectado con el, de tal maneira que a súa ausencia impediría ao produto realizar unha ou varias das súas funcións".

O art. 7 da proposta obriga os Estados a garantir que o fabricante dun produto defectuoso poida ser considerado responsable daqueles danos causados por ese produto e engade que, cando un compoñente defectuoso provocase que o produto sexa defectuoso, o fabricante dese compoñente tamén pode ser considerado responsable dos danos.

Do anterior cabe deducir que o fabricante dun sistema de IA, comercializado de forma autónoma, poderá ser considerado responsable con base na Directiva, grazas á inclusión expresa na definición de produto dos sistemas de IA autónomos.

Así mesmo, o fabricante dun equipo que incorpore un sistema de IA tamén poderá considerarse responsable dos posibles danos, cando sexa considerado defectuoso.

O fabricante que incorpore un compoñente ou un servizo conexo baixo o seu control tamén será considerado responsable. Xunto a el, o fabricante do compoñente ou servizo conexo que causou o defecto, tamén poderá ser considerado responsable solidario.

Por último, o art. 7.4 sinala que calquera persoa física ou xurídica que modifique un produto se considerará fabricante, cando a modificación sexa substancial. De tal maneira que, nos casos nos que o empresario realiza alteracións substanciais do equipo, será considerado fabricante e posible suxeito responsable para os efectos da Directiva. Non se consideran modificacións substanciais as simples actualizacións ou melloras do produto realizadas baixo o control do fabricante.

A partir de aquí, a Directiva trata de facilitar a carga da proba do prexudicado, de tal maneira que abonda con que probe o carácter defectuoso do produto, os danos sufridos e o nexo causal. Co fin de facilitar o carácter defectuoso do produto facúltase os órganos xurisdicionais nacionais a que, cando o demandante presentase probas suficientes da posible existencia do defecto, reclamen a exhibición de probas necesarias para valorar a existencia do defecto (art. 8 e 9 da proposta).

Conforme este réxime pódense reclamar os danos derivados de morte ou lesións corporais, incluídos os danos psicolóxicos, os danos derivados da perda ou corrupción de datos que non se utilicen con fins profesionais e os danos en calquera propiedade, salvo no propio produto defectuoso e en propiedades utilizadas con fins profesionais.

De forma paralela, tal e como se apuntou, a UE impulsou a Directiva sobre responsabilidade en materia de IA. Esta Directiva, tal e como recoñece no seu art. 1.3 b) non afecta os posibles dereitos que asistan aos prexudicados en virtude da Directiva de produtos defectuosos, que se acaba de analizar. O obxecto da Directiva é establecer normas comúns sobre todo en materia de carga da proba para as demandas de responsabilidade civil extracontractual subxectiva por danos e prexuízos causados por sistemas de IA. Trátase, por tanto, dunha norma que se basea na proba da culpa, non do defecto, pero que trata de facilitar a dita proba.

Con carácter xeral, o art. 4,1 sinala que se presumirá o nexo causal entre a culpa e os resultados producidos polo sistema de IA cando se dean as seguintes condicións: que se probou o incumprimento dun deber de dilixencia, que poida considerarse razoablemente probable que a culpa influíu nos resultados producidos polo sistema de IA, que a información de saída producida polo sistema de IA causou os danos.

No caso dos sistemas de IA de alto risco enténdese que se cumpre o requisito de non observación do deber de dilixencia cando non se observaron as obrigas recollidas nos capítulos 2 e 3 do proxecto de lei de IA. Establécense, ademais, unha

serie de obrigas para o provedor dun sistema de IA de alto risco, consistentes na achega de probas sobre o sistema de IA do que se sospeita que causou un dano, sempre que o demandante achegase indicios suficientes sobre a viabilidade da demanda (art. 3). Con todo, sinálase que non se aplicará a presunción cando o demandado demostre que o demandante pode acceder razoablemente a probas que demostran o nexo de causalidade (art. 4.4). No caso de sistemas de IA que non son de alto risco a presunción só se aplicará cando o órgano xudicial considere excesivamente difícil para o demandante demostrar o nexo causal (art.4.5). Por último, esta norma incorpora a previsión de posibles demandas por danos contra os usuarios de sistemas de IA de alto risco que, no caso de equipos destinados ao ámbito laboral, poderían ser os empresarios. Nestes casos entenderase que non observou o deber de dilixencia cando non cumpriu as obrigas previstas no art. 29, en concreto, non cumprir coas súas obrigas de utilizar ou supervisar o sistema de IA de conformidade coas instrucións, ou expoñer ao sistema a datos de entrada baixo o seu control que non eran pertinentes (art.4.3).

7. BIBLIOGRAFÍA

EU-OSHA: *Advanced robotics and automation: implications for occupationl safety and health,* 2022, dispoñible en: https://osha.europa.eu/en/publications/advanced-robotics-and-automation-implications-occupational-safety-and-health

EU-OSHA: *Artificial intelligence for worker management: an overview,* 2022, dispoñible en https://osha.europa.eu/en/publications/artificial-intelligence-worker-management-overview

EU-OSHA: *Artificial intelligence for worker management: mapping definitions, uses and implications,* 2022, dispoñible en: https://osha.europa.eu/en/publications/artificial-

intelligence-worker-management-mapping-definitions-uses-and-implications

GOÑI SEIN, J.L.: Ley de inteligencia artificial y seguridad y salud en el trabajo", en AA.VV. (dir.: Rodríguez Sanz de Galdeano, B. e Egusquiza Balmaseda, M.A.: *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.

BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital,* Wolters Kluwer, Madrid, 2019.

GOÑI SEIN, J.L.: *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018),* Bomarzo, 2018.

EGUSQUIZA BALMASEDA, M.A.: "Marco normativo general y propuestas de regulación en la responsabilidad civil" en AA.VV. (EGUSQUIZA BALMASEDA, M.A e RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.

JORQUI AZOFRA, M.: "El concepto legal de producto a la luz de la nueva propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos" en AA.VV. (EGUSQUIZA BALMASEDA, M.A y RODRÍGUEZ SANZ DE GALDEANO, B.): *Inteligencia artificial y prevención de riesgos laborales: obligaciones y responsabilidades,* Tirant lo Blanch, 2023, en prensa.