"NOTICIA SOBRE PROPOSTA DE REGLAMENT DE LA UNIÓ EUROPEA EN MATÈRIA D'INTEL·LIGÈNCIA ARTIFICIAL"

El repte d'establir límits jurídics al poderós, opac i irrenunciable mon digital

Per

CARLES VIVER PI-SUNYER

Comunicació per l'Acadèmia llegida en sessió ordinària de data 18 d'abril de 2023

I. PRESENTACIÓ

En aquesta comunicació pretenc únicament assenyalar els trets més fonamentals i fer una síntesi de la Proposta de Reglament sobre Intel·ligència Artificial (IA) elaborada per la Comissió Europea, que s'està tramitant actualment en el Parlament.

Es tracta d'un projecte normatiu important, per la transcendència, avui ja indiscutida, de l'objecte que regula, pel seu caràcter pioner i pel fet que es podria convertir, segons una opinió rellevant i força generalitzada[1], en un text de referencia per a altres regulacions. A això darrer hi contribuiria el seu abast supraestatal, la relativa equidistància que manté amb els models adoptats per les dues grans potències digitals[2], i el precedent del Reglament Europeu de Protecció de Dades, que ha jugat ja aquest paper de referent. És clara la necessitat de regular el més globalment possible un fenomen que és intrínsecament global; tot i que també ho és, de clara, la dificultat de bastir un referent compartit i, més encara, un referent global en un mon políticament polaritzat com l'actual. En tot cas, la Proposta de Reglament sembla voler assumir aquest rol quan en els "Considerants" inicials (equivalents al Preàmbul) proclama l'objectiu de convertit la Unió Europea en "un líder mundial" en l'àmbit de la IA[3].

Parteix de quatre premisses que revelen el context que la condiciona i que dona sentit a la regulació que proposa: a) l'impacte extraordinari que avui té la IA en "amplis sectors de l'economia i de la societat"[4], b) els beneficis irrenunciables que produeix en aquests

[1] No només a Europa sinó també fora del continent europeu. És el cas, entre altres, del llibre de H.Kissinger, E.Smith i D.Huttenlocher, *The Age of AI*, Ed. J.Murray, 2021, pag. 201.

[2] Tot i algunes propostes interessants, com la Recomanació sobre l'Ètica de l'IA de la Unesco, de novembre de 2022, ni Nacions Unides ni cap altra organització internacional està avui en condicions de desenvolupar aquest rol. Tampoc ho estan els dos Estats que lideren el mon de la IA, els EUA i la Xina: estan enfrontats en una lluita per l'hegemonia en un àmbit que ha assolit una importància econòmica, geo-estratègica i política extraordinària i tenen models de regulació i gestió radicalment diferents: el primer basat en el protagonisme de llibertat d'empresa, la regulació mínima i el proteccionisme radical, i la Xina amb un gran protagonisme de l'Estat en el desenvolupament i aplicació de la IA i una utilització guiada per l'objectiu primordial de controlar la societat.

[3] Diu concretament: "en un líder mundial en el desenvolupament d'una intel·ligència artificial segura, digna de confiança i ètica" (Considerant 5).

[4] Vid. Considerant 2.

àmbits[5], c) els riscos i dilemes, morals, filosòfics, socials i polítics que comporta[6] i, finalment, d) la necessitat de regular jurídicament aquest fenomen, i de fer-ho de manera equilibrada i orientada per valors i principis ètics i polítics. De fet, tant el Parlament com el Consell Europeu, quan van encarregar la redacció de la Proposta a la Comissió la van instar a que l'elaborés a partir de "principis ètics" [7].

El Reglament se suma a l'ampli consens existent avui sobre els canvis radicals que la IA provoca en una gran part de les activitats humanes. Uns canvis que alteren profundament la realitat -que ja no és únicament física sinó també cada cop més digital-, i fins i tot modifiquen la relació de la intel·ligència humana amb la realitat. Aquest fenomen es produeix sobretot des de l'aparició de sistemes d'IA capaços d'aprendre i de decidir de manera parcialment autònoma, és a dir, sense que els processos i regles que segueixen estiguin totalment prefixats per humans, i sovint sense que els seus programadors coneguin plenament el procediment emprat per aquests sistemes a l'hora de "raonar", aprendre[8] i decidir[9]-. La humanitat està delegant cada vegada més funcions i més rellevants a la IA[10] i ho està fent sense establir límits clars i eficaços. Històricament el mon s'havia interpretat, transformat i governat des de la fe o des de la raó humana associada a la ciència i la tecnologia. A partir de la aplicació generalitzada de la IA d'última generació, la intel·ligència humana està perdent el monopoli en la realització d'aquestes tasques fonamentals i, en un futur potser no llunyà, en molts àmbits podria quedar relegada a una posició en gran mesura subalterna respecte de la IA[11]. Els dilemes filosòfics i ètics que aquest escenari planteja són evidents. Es pot dir que està en joc el model de societat futur.

Tanmateix, sigui quina sigui la capacitat que finalment tingui la IA de substituir o de condicionar la intel·ligència humana, el fet cert és que ja avui una part important dels sistemes d'IA que s'estan aplicant posen ja en risc valors, principis, drets, bens i interessos públics i privats de tota mena; com a conseqüència, entre altres, d'errors en

[5] Que concreta en el Considerant 3 fent referència al medi ambient, la assistència sanitària, l'agricultura, l'educació, l'administració d'infraestructures, l'energia, el transport, la logística, els serveis públics, la seguretat, la justícia, l'eficiència dels recursos, la mitigació del canvi climàtic i, de manera especial, les "avantatges competitives essencials per a les empreses".

[6] Considerants 1, 4 i 5.

[7] Es tracta de la Resolució del Parlament Europeu de 20 d'octubre de 2020 que insta la Comissió a fer la Proposta de Reglament i conté les "recomanacions adreçades a la Comissió sobre un marc dels aspectes ètics de la IA, la robòtica i les tecnologies connexes -2020/20112 (INL)". En sentit similar es va pronunciar el Consell Europeu en la Reunió Extraordinària de 1 d'0ctubre del mateix any.

[8] En serien exemples rellevants el sistema denominat d'aprenentatge profund, que processa la informació de manera similar a com hi fa la xarxa neuronal del cervell humà -p.e., amb estratègies de raonament per inferència-; o els d'aprenentatge per reforç que aprenen per si sols a base de recompensa-penalització (prova-error).

[9] En serien exemple els sistemes que imposen multes, venen accions borsàries, condueixen cotxes o decideixen objectius i atacs militars.

[10] En són exemples els sistemes denominat generatius, com p.e. el ChatGPT, els quals, a partir d'una sol·licitud oral o escrita, generen de manera immediata tota mena de textos, imatges, vídeos o sons d'alta qualitat difícils de diferenciar dels generats per humans.

[11] Vegeu H.Kissinger et alii, *ob. cit.*, pàg. 29 i s.

les dades que empren, de deficiències en el disseny dels algoritmes[12], de biaixos discriminatoris que sovint incorporen[13] o, simplement, de la vulnerabilitat de determinats col·lectius als quals s'apliquen.

Des de l'ètica fa temps que es proposen límits als sistemes d'IA. En treballs de prestigiosos Instituts Universitaris, d'organitzacions no governamentals i de comitès empresarials d'ètica proliferen estudis, declaracions, codis ètics i guies de bones pràctiques. És imprescindible que es mantingui viu el debat ètic i filosòfic tant en la seva dimensió o enfocament global com del aplicat a riscos concrets. Tanmateix, la magnitud dels riscos que generen aquests sistemes fa imprescindible fer un pas endavant i transformar els principis i valors ètics i polítics en regles jurídiques d'obligat compliment, que certament han d'anar compassades en tot moment amb el debat ètic, i s'han de guiar pels objectius primordials de garantir l'autonomia i la dignitat de les persones[14] i de la prevalença de la intel·ligència humana en la interpretació, transformació i govern de la realitat. Així ho reconeix la Proposta tot identificant, de manera reiterada, com a bens a protegir "la seguretat, la salut i els drets fonamentals incorporats al Dret de la Unió". El que no inclou l'articulat, potser per pragmatisme jurídic, són els valors de la Unió[15]; tot i que s'esmenten en el preàmbul i, a més, en les esmenes a la Proposta presentades en el Parlament es proposa incorporar aquests valors a una dotzena d'articles.

Amb tot, malgrat el reconeixement cada cop més extens de la necessitat de regular jurídicament la IA, són comptats els estats que han dictat una regulació general sobre aquesta matèria.[16]. De fet, la regulació jurídica possiblement no és l'únic instrument ni el més decisiu a l'hora de fer front als riscos esmentats. Probablement seria més rellevant el paper de filtre protector que podria desenvolupar, p.e., una sòlida, malgrat que improbable, formació política i, sobretot, una formació moral crítica de la ciutadania. Tanmateix, la regulació jurídica és avui imprescindible i fins i tot urgent. Es podria recordar aquí la recent carta oberta signada per més d'un miler d'acadèmics, experts i empresaris del sector demanant, entre altres, una pausa de sis mesos en el

[12] A base, p.e., de simplificar en excés qüestions complexes a l'hora de l'avaluar i classificar les dades emprades, de programar i entrenar les classificacions de les relacions entre elles o d'inferir els patrons que utilitzen per obtenir els resultats.

[13] Racials, culturals, socio-econòmics, de gènere, etc. Per una anàlisi, molt interessant, a partir de casos concrets, sobre la manera en la que els algoritmes produeixen tècnicament els biaixos i com es podrien evitar, vegeu Agència Europea pels Drets Fonamentals "Bias in Algorithims. A.I.and Discriminatio".

[14] Sobre aquesta qüestió, vegeu, p.e., la *Declaració sobre IA, robòtica i sistemes "autònoms"* del Grup Europeu sobre Ètica de les Ciències i les Noves Tecnologies, de la Comissió Europea, de 9 de març de 2018.

[15] Són els de respecte de la dignitat humana, la llibertat, la igualtat, la democràcia, Estat de Dret i els drets humans.

[16] Entre aquests comptadíssims Estats hi ha la Xina i alguns estats dels EUA com Texas, Califòrnia, Florida. Al Brasil la llei d'IA està en tràmit en el Senat (febrer 2023).

desenvolupament de sistemes -tot i que amb una finalitat no totalment altruista-, o també la prohibició a Itàlia *del famós* ChatGPT[17]. Però prohibir és més fàcil que regular.

Regular els sistemes d'IA és molt complicat degut a la complexitat tècnica, les constants innovacions i l'opacitat d'aquests sistemes; a la resistència de les potents empreses tecnològiques del sector a qualsevol mena de regulació; i també a la necessitat imperiosa que els límits jurídics no posin traves innecessàries a unes tecnologies que estan contribuint de manera decisiva al desenvolupament econòmic, científic, social, cultural i fins i tot polític o de governança pública. Cal trobar l'equilibri entre la banalització inconscient d'uns riscos que són reals i la estigmatització d'uns sistemes actualment irrenunciables.

En aquest sentit la Proposta declara la voluntat de fer compatible "el desenvolupament, la comercialització, l'ús i la innovació constant de la IA", mitjançant l'establiment d'un marc jurídic uniforme que millori el funcionament del mercat únic europeu[18], amb la protecció de la salut, la seguretat i els drets fonamentals reconeguts en el Dret de la Unió, mitjançant normes que limitin els sistemes d'IA a partir dels principis ètics i polítics de la Unió Europea. Es tracta de dos objectius que, segons el Reglament, no són necessàriament antagònics sinó que poden potenciar-se mútuament: una IA respectuosa amb els principis ètics i polítics de la UE és més confiable i per això mateix potencialment més acceptada i, finalment, econòmicament més rendible. Abans però d'analitzar com es pretén trobar aquest punt d'equilibri, vegem en quin estadi es troba la tramitació de la Proposta.

II. ESTAT DE LA TRAMITACIÓ

A 15 d'abril de 2023, a més de la Proposta de la Comissió[19], han presentat ja les seves propostes, provisionals però molt completes i elaborades, el Parlament i el Consell Europeu: el Parlament a través del preceptiu "Projecte d'Informe" de la Comissió Conjunta del Parlament competent per raó de la matèria (en endavant C.C.)[20] i mitjançant les Opinions i esmenes presentades per les 7 comissions parlamentàries amb

[17] L'Estat espanyol està ponderant la possibilitat de prohibir aquest sistema.

[18] Considerants 1, 5 i 71. La Proposta no preveu cap altra política o mesura específica rellevant com podria ser el foment de la capacitat dels poders públics de dissenyar i desenvolupar sistemes propis per tal de no dependre tant com ara del sector privat (com defensa M.Mazzucato, "IA in the Common Interest", *Project Syndicate. New York Times, de 26 de desembre de 2022*) o per tal que els beneficis que genera la IA arribin a sectors socials als quals altrament no arribarien per manca d'interès del sector privat (com sosté Bill Gates. Blog personal *Gates Notes,* 21 març 2023).

[19] La Proposta consta d'una Exposició de Motius, uns Considerants o preàmbul, un text articulat de 85 articles -llargs i amb força remissions internes i externes-, un Fitxer Financer i nou Annexes.

[20] Es tracta d'un Informe important que, a més d'una il·lustrativa exposició de motius, conté 46 esmenes als Considerants i 263 a l'articulat. La C.C., creada per a la ocasió, la conformen la Comissió de Mercat Interior i la de Llibertats Civils, Justícia i Afers Interiors.

dret a fer-ho[21]; el Consell mitjançant un document exhaustiu i detallat presentat el desembre de 2022 que incorpora millores de tècnica legislativa, que afecten la sistemàtica, la precisió i la completesa de la Proposta, i algunes esmenes de fons que han de servir, segons el Consell, de "base per preparar les negociacions amb el Parlament". La tramitació de la Proposta, que es va iniciar l'abril de 2021[22] i que segueix el procediment legislatiu ordinari, es troba en aquest moment en la fase d'obertura del debat i votació de les esmenes en el si de la C.C. Es pot afirmar, però, que les cartes a jugar són ja sobre la taula.

III. OBJECTE REGULAT

El Reglament estableix normes harmonitzades, i d'unificació del mercat europeu, en les quals es regulen els requisits que han de complir els sistemes d'IA per entrar en aquest el mercat i per posar-s'hi en funcionament[23]. La regulació té una clara vocació d'exhaustivitat, que es manifesta en l'objectiu declarat de "impedir que els Estats membres imposin restriccions al desenvolupament de la IA, llevat que el Reglament ho autoritzi expressament" [24]. A tal efecte s'estableix una mena de "reserva de normació europea" a favor de la Comissió[25], que a la pràctica pot limitar de manera significativa la futura capacitat normativa dels Estats membre en aquest àmbit. L'Informe del Consell europeu reforça encara més la idea de reserva normativa a favor de la Unió tot regulant amb més detall la part procedimental i orgànica de la Proposta i obligant la Comissió a adoptar més actes normatius i executius de desenvolupament del Reglament.

---

[21] Són les Comissions de Industria, Cultura, Medi Ambient, Transports i Afers Jurídics, a més de les dues Comissions que conformen la C.C. Han presentat a la C.C. 3.312 esmenes (779 als Considerants i 2.533 a l'articulat).

[22] Prèviament, tant la Comissió EU com el Parlament havien produït treballs que es podrien qualificar de preliminars. Destaquen els preparats pel Grup d'experts d'alt nivell sobre IA: "Directrius ètiques per a una IA fiable" (2019); el Llibre Blanc sobre IA: un enfoc europeu orientat a l'excel·lència i la confiança, de la Comissió EU (2020); la Resolució del Parlament sobre aspectes ètics de la IA, la relativa a la responsabilitat civil en matèria d'IA, la Resolució sobre drets de propietat intel·lectual i IA (totes tres d'octubre de 2020), i els Projectes d' Informes sectorials sobre ús de l`IA en àmbits penals, educació, cultura i audiovisuals (2020).

Durant l'any 2001 van presentar els corresponents Dictàmens preceptius: el Banc Central Europeu, el Comitè Europeu de les Regions, el Comitè Europeu Econòmic i Social, algunes Cambres s Parlamentaries dels Estats membres i la Oficina Conjunta del Comitè i del Supervisor Europeu de Protecció de Dades.

[23]Per entrada en el mercat s'entén la "primera comercialització" i per posada en funcionament el "primer d'us" per part d'un usuari.

[24] Considerant 1.

[25] Els àmbits reservats fan referència, entre altres, a la normativa necessària per adaptar el Reglament als canvis que experimenti la IA, per establir regulació provisional i supletòria, per modificar normativa existent i també per establir orientacions i models que facilitin el compliment de requisits i obligacions imposades pel Reglament. Aquesta normació que la dictarà la Comissió mitjançant els actes delegats de l'article 73. Com veurem més endavant, a aquestes facultats normatives de la Comissió se'n afegeixen nombroses d'executives.

Amb aquesta mateixa vocació d'exhaustivitat, la Proposta parteix d'un concepte molt ampli de sistema d'IA. Concretament el defineix com: qualsevol software o programa informàtic, incorporat en un robot o "independent", que, per tal d'assolir objectius fixats per essers humans[26], empra qualsevol de les estratègies d'aprenentatge automàtic, tècniques estadístiques o estratègies basades en la lògica i el coneixement que figuren de manera oberta, per via d'exemple a l'Annex I[27], per tal de produir com a resultat "continguts[28], prediccions, recomanacions o decisions". És clara la voluntat de no excloure ex *ante* cap programa informàtic capaç de processar dades tot emulant els processos de raonament de la intel·ligència humana. O dit d'una altra manera: és clar l'objectiu d'incloure com a potencial objecte de prohibició o de regulació qualsevol dels sistemes d'IA existents o que es puguin crear en el futur[29].

Aquesta opció per un concepte ampli -i potencialment indeterminat- de sistema respon un motiu molt rellevant. Respon a la utilització del criteri de risc com a criteri per delimitar l'objecte de regulació, enlloc del criteri del tipus de sistema utilitzat: el Reglament s'aplica a qualsevol sistema capaç de produir algun dels riscos que tipifica. La Proposta sembla dir: atesa la inabastable multiplicitat de tècniques emprades per la IA i la seva constant i accelerada innovació, m'és indiferent el tipus de sistema que s'utilitzi: si produeixi o pot produir els riscos que identifico, serà objecte dels límits que estableixo.

A partir d'aquest criteri, que ha merescut el beneplàcit general, es distingeix tres categories de riscos als quals vincula tres tipus de conseqüències jurídiques: a) els riscos radicalment inassumibles, que donen lloc a la prohibició de les pràctiques o sistemes d'IA que els poden generar; b) els sistemes considerats de risc alt, que no es prohibeixen però que se sotmeten a límits estrictes en forma de requisits i obligacions; i c) els riscos capaços de generar; a') confusió sobre "l'autenticitat o veracitat" d'imatges, sons, i vídeos creats artificialment; a') els riscos derivats de l' incertesa de si hom està interactuant amb una màquina o amb una persona; i c') els riscos associats al reconeixement d'emocions i a la categorització biomètrica de persones. En aquests tres últims supòsits tan sols s'imposen obligacions de transparència[30]. Per a la resta de

[26] No existeixen encara sistemes que puguin fixar els seus propis objectius ni de realitzar funcions generals indeterminades. És cert, però, que alguna de les empreses tecnològiques ha iniciat treballs de creació d'aquests sistemes que es qualifiquen de sistemes IA general. Si s'arribessin a crear, es produiria un canvi radical en el mon de la IA (vegeu Bill Gates, art. cit.)

[27] En la primera categoria inclou *ad exemplum,* entre altres*,* l'aprenentatge supervisat, el no supervisat, el de reforç o l'aprenentatge profund; en la segona, la representació de coneixements, la programació lògica inductiva; i en la tercera els mètodes de cerca i optimització.

[28] Concretament: textos, imatges, vídeos i sons.

[29] De fet, a l'art. 4 s'habilita la Comissió per tal que modifiqui el llistat de l'Annex a fi d'adaptar-lo "als avenços tecnològics".

[30] Vegeu l'article 52.

sistemes el Reglament es limita a recomanar l'elaboració del que denomina de "Codis de conducta"[31].

En relació a aquest plantejament el Consell Europeu fa dues precisions: limita el concepte de sistema d'IA i, en conseqüència, l'objecte regulat, als sistemes que funcionen amb elements d'autonomia, és a dir, excloent els sistemes que empren només regles definides per persones físiques; i, en segon lloc, preveu un tractament especial -que la Comissió establirà- pels sistemes que denomina "d'ús general", que defineix de manera oberta[32]. Les dues precisions poden considerar-se en principi raonables, tot i que, paradoxalment, poden augmentar la inseguretat que pretenen evitar: en superposar al criteri de risc un criteri de naturalesa diferent emprant, a més, criteris força indeterminats, sobre tot el segon.

IV. ÀMBIT D'APLICACIÓ. EXCLUSIONS

L'àmbit d'aplicació, que contribueix a precisar l'objecte regulat, respon d'entrada a la voluntat de garantir la "protecció de la **sobirania digital de la UE** "[33], que es concreta en la decisió d'aplicar el Reglament a: a) als proveïdors de qualsevol sistema introduït o posat en servei en el territori de la Unió amb independència de si estan establerts o no en territori de la Unió[34], b) als usuaris que es trobin a la Unió i c) als proveïdors i usuaris que es trobin en un tercer país quan la "informació de sortida" del sistema (és a dir el "contingut" generat) s'utilitzi en el territori de la Unió (art.2.1)[35]. Amb tot, a diferencia del que succeeix en alguns estats, la sobirania digital no inclou prohibicions d'entrada de sistemes forans pel sol fet de ser-ho ni restriccions a l'exportació per aquest fet.

L'aplicació general del Reglament té, però, cinc exempcions importants:

No s'aplica a "les autoritats públiques de tercers països ni a les organitzacions internacionals" que utilitzin els sistemes en el marc d'acords internacionals, subscrits amb l'UE o amb algun dels Estats membres!!, amb fins de l'aplicació de les lleis relatives a infraccions penals, a l'execució de sancions penals o a la cooperació judicial (art. 2.4).

[31] Adreçats a promoure l'aplicació voluntària dels requisits exigits als sistemes d'alt risc a aquests sistemes. Afegeix que la Comissió fomentarà i facilitarà l'elaboració d'aquests codis de conducta, especialment en relació als proveïdors a "escala petita" i les empreses emergents.

[32] Com a sistemes que "poden utilitzar-se en una pluralitat de contextos i de sistemes, ...**com els de** reconeixement d'imatge o veu, generació d'àudio i vídeo, reconeixement de patrons, resposta a preguntes i traducció".

[33] Punt 2.2. de l'Exposició de Motius.

[34] S'exceptuen, però, els sistemes d'us personal.

[35] La C.C. proposa que els obligats de la lletra a) siguin tots els que participin en la cadena de valor i que a la lletra c) s'afegeixi el supòsit de la informació que "afecti les persones físiques en la UE".

Tampoc s'aplica als "sistemes desenvolupats o emprats amb fins exclusivament militars" (art.2.3). L'exclusió és rellevant[36] i ha sigut criticada[37].

A més, hi ha cinc àmbits als quals no se'ls hi aplicarà el Reglament "mentre no ho prevegi la Comissió" (art. 2.2). Són àmbits en els quals hi ha vigents reglaments i directives de la Unió que, de moment, es consideren suficients per garantir l'aplicació dels límits previstos en el Reglament[38].

Finalment, i molt important, el Reglament estableix que no s'aplicarà fins passats els dos anys de la seva entrada en vigor, i que, passats aquests dos anys, pel que fa als sistemes introduïts en el mercat abans d'aquesta data, només se'ls hi aplicarà si experimenten en el futur "canvis significatius" en el disseny o la finalitat (art.83.2). Aquesta inaplicació s'allarga a tres anys en el cas dels sistemes establerts en virtut de la legislació europea relativa al denominat espai de llibertat, seguretat i justícia[39] (art. 83.1) [40]. Aquestes "moratòries", possiblement justificades des d'un punt de vista pragmàtic, poden comportar la inaplicació del Reglament a un nombre elevat dels sistemes que s'aplicaran a la UE durant força temps[41]. Caldria deixar clar quin procediment s'aplicarà per comprovar si s'han produït els canvis significatius al·ludits [42] i, sobretot, caldria aplicar-lo de manera rigorosa.

V. PRÀCTIQUES PROHIBIDES

El Reglament només prohibeix tres tipus de "pràctiques". Les prohibicions responen al triple objectiu d'impedir la manipulació de persones, la discriminació de persones i col·lectius i el control social mitjançant vigilància indiscriminada. Concretament es prohibeixen:

---

[36] En tractar-se de sistemes d'última generació que han modificat radicalment tant les estratègies militars com l'armament físic i cibernètic emprat, multiplicant la seva capacitat d'atac i de defensa, i els riscos pels drets i llibertats.

[37] El Consell Europeu pretén justificar-la pel fet que existeix ja una regulació militar.

[38] Són els àmbits de seguretat de l'aviació civil; dels vehicles agrícoles o forestals; dels vehicles a motor de dues, tres o quatre rodes i remolcs; dels equips marins i dels sistemes ferroviaris.

[39] Són concretament els Reglaments integrats en els sistemes d'informació aplicats a la legislació relativa a l'espai Schengen; a visats; a comprovació de dades biomètriques, identificació de nacionals de tercers països; entrades i sortides; autorització de viatges; antecedents penals de nascuts en tercers països i apàtrides; i inter-operatividad dels sistemes d'informació en l'àmbit de fronteres i visats, cooperació policial i judicial i d'asil i migració.

[40] El Consell Europeu proposa afegir a la llista de sistemes exclosos els que tenen fins únicament d'investigació i desenvolupament científic.

[41] En tot cas, a banda dels efectes de la "moratòria", segons Melissa Heikkila, "A quick guide to the most important AI law you've never heard of", a *MIT Tecnology Review* 2 de juny de 2022, la "UE" (sic) sosté que els sistemes prohibits o sotmesos als requisits establerts en el Reglament només seran entre un 5 i un 15% dels sistemes aplicats a la Unió.

[42] Possiblement seria el procediment previst en el Títol VIII dedicat al "Seguiment posterior a la comercialització", però no és evident que sigui així.

a) els sistemes capaços d'alterar, a través de tècniques subliminals[43], el comportament de les persones -especialment les que pertanyen a grups vulnerables per raó d'edat o discapacitat- i sempre que l'alteració "provoqui o sigui provable que provoqui" perjudicis físics o psicològics[44]. Aquesta darrera exigència acota l'abast del concepte d'alteració del comportament, que altrament s'aplicaria a una gran part dels sistemes d'IA, atès que habitualment emmagatzemen i tracten dades personals amb la finalitat d'orientar, influir, condicionar i sovint manipular futures conductes. Amb tot, caldrà veure com s'interpreta i aplica el criteri de probabilitat i el concepte de perjudici des de la perspectiva tant del seu abast com de la uniformitat.

b) els sistemes utilitzats per les autoritats públiques per classificar les persones[45] en funció de la conducta social o les característiques personals, quan la classificació social provoqui tractes perjudicials o desfavorables en contextos socials diferents dels que van generar les dades o quan els tractes perjudicials siguin injustificats o desproporcionats en relació al comportament social de les persones afectades. També en aquest cas caldrà precisar l'abast de la prohibició i garantir la seva aplicació uniforme a tota la UE.

c) el darrer supòsit és concret i específic, però és el que ha suscitat més polèmica per l'excepció que inclou. És la prohibició de l'ús per part de les autoritats públiques de sistemes d'identificació biomètrica (de les característiques físiques o de conducta), "remota" (feta a distància), en "temps real" (sense dilació entre la recollida de les dades i la identificació), en espais oberts, i amb la finalitat d'aplicar la legislació penal [46].

Aquesta prohibició té, però, una excepció: no es prohibeixen aquests sistemes quan la esmentada identificació sigui "estrictament necessària" per "cercar víctimes d'un delicte..., prevenir una amenaça...per a la vida o la seguretat física o un atemptat terrorista o per a la detecció...de persones que hagin comés o se sospiti que han comés (determinats) delictes...pels quals s'imposin penes privatives de llibertat de com a mínim tres anys " [47].

En aquests casos es poden usar aquests sistemes però la seva aplicació se sotmet al compliment d'alguns requisits estrictes, que, tanmateix, admeten excepcions. És el supòsit, p.e., l'exigència de l'autorització prèvia judicial o d'una "autoritat administrativa

[43] Que transcendeixen la consciència de la persona.

[44] Com serien els casos, no infreqüents, dels relacionats amb anorèxies, autòlisis o suïcidis.

[45] Cal recordar que la classificació és una estratègia d'ús habitual per part dels algoritmes.

[46] Concretament, l'art. 3.41 del Reglament, entén per legislació penal "les activitats realitzades per les autoritats encarregades de l'aplicació de la legislació per a la prevenció, investigació, detecció o enjudiciament d'infraccions penals o execució de sancions penals".

[47] Concretament, segons l'art. 5.d), la identificació es pot aplicar quan sigui "estrictament necessària per... cercar possibles víctimes d'un delicte; ...prevenir una amenaça específica, important i imminent per a la vida o la seguretat física o un atemptat terrorista o per a la detecció, localització, identificació o enjudiciament de persones que hagin comés o se suposi que han comés algun dels (32) delictes recollits a l'article .2.2 de la Decisió Marc 2002/584 del Consell" (relativa a l'ordre de detenció i als procediments de lliurament de persones entre Estats membres), per els quals la normativa de l'Estat membre implicat imposi penes de com a mínim tres anys.

independent", que en cas d'urgència justificada es pot sol·licitar de manera simultània o posterior al seu ús.

Cal destacar, però, que el Reglament[48] deixa en mans dels Estats l'opció de no incorporar a la seva legislació la possibilitat d'aplicar el control policial biomètric referit. És una mena d'*opting out*, que debilita la finalitat uniformitzadora del Reglament i que possiblement pretén mitigar les crítiques que l'esmentat control havia suscitat en alguns Estats de la Unió mentre s'elaborava la Proposta. La resta de sistemes d'identificació biomètrica són considerats de risc alt i sotmesos a requisits específics.

VI. SISTEMES DE RICS ALT

VI.1 *Identificació*

El Reglament identifica els sistemes de risc alt, de manera taxada, en dues llistes[49]. En la primera s'inclouen 18 sistemes caracteritzats per: a) ser components de seguretat de determinats "productes" o productes en sí mateixos (màquines, robots, drons...); b) ser capaços de provocar riscos per a la salut, la seguretat o els drets fonamentals; i c) estar regulats en disposicions europees sobre protecció de la salut o la seguretat que exigeixin, entre altres, una avaluació de la conformitat per part d'un organisme independent[50].

En la segona[51] hi figuren 21 sistemes "independents" (és a dir no integrats "productes"), que comporten riscos per determinats drets fonamentals de la Unió, que es descriuen en cada cas. S'agrupen en els 8 àmbits o matèries següents:

- El de la identificació biomètrica i caracterització de persones, que inclou els sistemes d'identificació biomètrica remota en temps real o diferit no prohibits per l'art. 5[52].

- El de la gestió i funcionament d'infraestructures essencials: els emprats en la gestió del transit rodat i el subministrament d'aigua, gas, calefacció i electricitat[53].

---

[48] Ho fa en el darrer punt d'aquest article i amb una redacció confusa, que tanmateix es podria considerar aclarida a la llum del Considerant 22.

[49] Art. 6.1 amb remissió als Annexes II i III.

[50] Es tracta de la legislació sobre seguretat de joguines, màquines, embarcacions, ascensors, aparells que usen atmosferes potencialment explosives, equips radioelèctrics, equips a pressió, instal·lacions de transport per cable, equips de protecció individual, aparells que cremen combustibles gasosos, productes sanitaris i productes sanitaris per diagnosi *in vitro.* A aquesta llista s'afegeix la legislació relativa als cinc àmbits citats a la nota 38 (sistema de seguretat de l'aviació civil, del sistema ferroviari...).

[51] Art. 6.2 i Annex III.

[52] Segons el Considerant 33 les possibles imprecisions tècniques d'aquests sistemes poden donar resultats esbiaixats i tenir conseqüències discriminatòries (per raó de sexe, edat, ètnia...). Cal aplicar-los-hi requisits específics pel que fa a la capacitat de registre i de vigilància humana.

[53] Atès que, segons el Considerant 34, un funcionament defectuós pot produir perills per a la salut, la seguretat o alterar de manera apreciable activitats econòmiques i socials.

- El d'educació i formació professional: els sistemes utilitzats per determinar l'accés a centres educatius i de formació professional o per avaluar els resultats dels aprenentatges dels alumnes[54].

- El d'ocupació i gestió de treballadors i accés a l'autoocupació: els emprats per a la contractació, selecció, promoció, assignació de tasques, avaluació de rendiments dels treballadors[55].

- El de l'accés i ús de serveis públics i privats: els emprats per les autoritats públiques per avaluar l'accés o l'accés prioritari als serveis públics (bombers, assistència mèdica...), per a l'accés i gaudi de serveis i ajudes essencials de caràcter públic i privat com el crèdit -mitjançant la qualificació creditícia o solvència de persones físiques-, o l'accés a l'habitatge, l'electricitat i les telecomunicacions en situacions d'emergència.[56]

- El d'afers relacionats amb "l'aplicació llei": els emprats per autoritats públiques per tal d'avaluar els riscos de comissió d'infraccions penals i de reincidència; la utilització de polígrafs i detecció d'estats emocionals; l'avaluació de la fiabilitat de les proves durant la investigació o l'enjudiciament d'infraccions penals i l'elaboració de perfils de persones físiques en l'àmbit de les investigacions penals[57]. Cal destacar que la C.C. ha presentat una esmena adreçada a incloure els sistemes d'aquest àmbit entre les pràctiques prohibides. Argumenta que "l'actuació policial predictiva viola la dignitat humana i la presumpció d'innocència, i comporta un risc particular de discriminació... vetat en les societats liberals"[58].

- El de gestió d'immigració, asil i control fronterer: la utilització de polígrafs i detecció d'estats d'emocionals; l'avaluació dels riscos per a la seguretat o la salut que pot generar una persona que pretén entrar il·legalment en el territori d'un Estat membre, així com els sistemes per verificar l'autenticitat de documents en aquest àmbit[59].

[54] Poden decidir la trajectòria formativa i professional. Poden violar el dret a l'educació o a no patir discriminació i perpetuar patrons històrics de discriminació (Considerant 35).

[55] Poden afectar perspectives laborals i de subsistència. Poden perpetuar patrons històrics de discriminació de les dones, de determinats grups d'edat, de discapacitats, o per l'origen racial o ètnic o la orientació sexual. Poden afectar drets de protecció de dades personals i privacitat (Considerant 36).

[56] Poden discriminar persones o grups socials i vulnerar drets com a la dignitat humana, a la tutela judicial, la vida o la salut (Considerant 37).

[57] Poden donar lloc a vigilància, detenció i privació de llibertat i afectar drets fonamentals com la tutela judicial, al jutge imparcial, a la defensa o a la presumpció d' innocència. No es consideren, però, de risc alt els sistemes emprats per autoritats fiscals i duaneres en processos administratius utilitzats per prevenir, investigar i enjudiciar infraccions penals (Considerant 38).

[58] Vegeu l'esmena 76 i l'Exposició de motius.

[59] Poden vulnerar drets de lliure circulació, no discriminació, intimitat personal, protecció dades, protecció internacional i bona administració (Considerant 39).

- I l'àmbit d'Administració de justícia i processos democràtics que inclou els sistemes dirigits a " ajudar les autoritats judicials en la investigació i interpretació de fets i de la llei"[60].

A aquests sistemes la C.C. hi afegeix o especifica , crec que amb bon criteri: els sistemes que poden influir en el desenvolupament dels infants; els emprats per candidats i partits en les eleccions locals, nacionals i europees i en la comptabilització dels vots; el triatge de pacients en el sector sanitari; l'accés a assegurances de salut i vida; les ultra-falsificacions que suplanten personatges reals i els continguts editorials escrits amb IA ("autors d'IA").

Finalment, com a clàusula de tancament, la Proposta (art. 7.1) atorga a la Comissió "poders per adoptar actes delegats" per tal que pugui anar afegint al llistat de sistemes de risc alt, sistemes incloibles dins d'algun dels 8 àmbits taxats esmentats, que comportin un risc per a la salut, la seguretat o els drets fonamentals "d'una gravetat i probabilitat equivalents o superiors" a la dels sistemes inclosos en la llista referida[61]. És més, l'obliga a avaluar la necessitat de modificar el llistat un cop a l'any a partir de l'entrada en vigor del Reglament (art. 84.1). A l'art. 7.2 estableix els criteris que haurà de tenir en compte la Comissió en avaluar la integració d'un nou sistema en la llista de risc alt.

D'aquesta regulació sembla deduir-se voluntat, manifesta en els Considerants, d'acotar de manera "clara" l'abast dels sistemes considerats de risc alt. Tanmateix, els enunciats dels 8 àmbits en els quals es poden afegir sistemes de risc alt i la mateixa definició de l'abast d'aquest risc són força indeterminats. Caldrà veure també aquí si a la pràctica el sistema de governança i els procediments de seguiment previstos a la Proposta garanteixen una interpretació i aplicació prou uniforme i jurídicament segura.

Un cop identificats els sistemes de risc alt, el Reglament en regula cinc aspectes fonamentals : a) els requisits que han de complir els sistemes; b) les obligacions dels operadors; c) el procediment d'avaluació de la conformitat al qual s'han de sotmetre; d) els organismes i autoritats encarregades de garantir l'aplicació i execució del Reglament i els procediments de vigilància del mercat i de control dels riscos que generin amb posterioritat a la posada en servei; i e) el règim sancionador. Vaguem-ne els aspectes més rellevants:

VI.2 *Requisits que han de complir els sistemes de risc alt*

[60] Poden afectar "la democràcia, l'Estat de Dret, les llibertats individuals i el dret a la tutela judicial efectiva i al jutge imparcial", en particular "els sistemes que ajuden les autoritats judicials a investigar i interpretar els fets i el Dret i a aplicar la llei als casos concrets". S'exclouen els sistemes relatius a "les activitats administratives accessòries que no afecten l'administració de justícia en casos concrets" (Considerant 40).
[61] En el considerant 27 s'afirma que "aquesta limitació restringeix al mínim qualsevol possible restricció al comerç internacional".

Els sistemes han de complir 7 requisits que es regulen amb detall. Es poden sintetitzar així:

1r) Han d'incorporar un sistema de gestió de riscos, que s'aplicarà durant tot el cicle de vida i contindrà la identificació de riscos coneguts i previsibles, i les mesures adequades per a gestionar-los[62].

2n) En els sistemes que empren tècniques d'entrenament de models amb dades, s'han de sotmetre a un seguit de pràctiques, com l'examen previ de possibles biaixos, la detecció de llacunes, i l'avaluació de la quantitat i adequació de les dades. A més, les dades emprades han de complir requisits estrictes, com la pertinència i representativitat, la absència d'errors, la completesa i l'adequació de les propietats estadístiques. La C.C., "a instancies de la industria", proposa convertir els requisits d'absència d'error i de completesa en un objectiu a assolir "en la mesura del possible"[63]. Una part important dels comentaristes del Reglament advertia ja la necessitat introduir aquesta matisació, que no deixa de ser significativa.

3r) Han d'incorporar, abans de la introducció en el mercat o la posada en funcionament, i al llarg de tota la seva vida, la documentació tècnica que demostra que compleixen els requisits exigits[64].

4r) Han de garantir la traçabilitat del funcionament del sistema mitjançant arxius de registre automàtic de "esdeveniments".

5è) El disseny i el desenvolupament han de garantir un nivell de transparència "suficient" i una comunicació d'informació que permeti que els usuaris puguin interpretar i utilitzar correctament la informació de sortida. La transparència és un requisit clau per garantir els drets fonamentals; cal notar, però, la contenció amb la que es regula el nivell de transparència i d'informació exigit[65]. És clar que aquí hi juga, com a contrapunt limitador, els drets d'autor, de propietat intel·lectual, la llibertat de les arts i les ciències, i la llibertat d'empresa.

6è) S'han de dissenyar i desenvolupar de manera que puguin ser vigilats per persones, capacitades per intervenir en el funcionament dels sistemes i, si escau, per interrompre'l[66]. És un requisit summament important per a limitar els perills dels

[62] L'art. 9 descriu el contingut que han de tenir els sistemes i les pautes que han de tenir en compte els proveïdors a la hora de dissenyar les mesures de gestió. Els sistemes de gestió s'hauran de sotmetre a procediments de prova en el moment de l'entrada en el mercat i al llarg de tot el cicle de vida dels sistema.
[63] Esmena 96 a l'art. 10.3. de la Proposta.
[64] Entre els que destaca la "descripció detallada" dels elements cabdals del sistema i del seu desenvolupament, com ara: els mètodes adoptats pel desenvolupament, la lògica general del sistema i dels algoritmes incorporats, persones o grups de persones amb les que es preveu que es relacioni o les opcions de classificació emprades (vegeu, Annex IV de la Proposta).
[65] El Considerant 47 afirma que "cal exigir **un cert grau** de transparència".
[66] En el cas dels sistemes d'identificació biomètrica s'exigeix la vigilància de dues persones com a mínim.

sistemes que aprenen o decideixen autònomament i per assegurar la que s'ha qualificat com a "reserva d'humanitat"[67].

7è) S'han de dissenyar i desenvolupar de manera de funcionin amb un "nivell adequat" de precisió, solidesa i, molt important, han d'estar protegits contra els ciber-atacs cada vegada més freqüents i més perillosos pels drets fonamentals. per tal d'evitar, entre altres, vulneracions massives de la privacitat [68].

A més d'aquests 7 requisits, els sistemes han de complir els requeriments que els hi imposen altres normes europees que regulen matèries que incideixen en aspectes específics de la IA, com destacadament la legislació sobre protecció de dades, entre moltes altres[69]. El Reglament regula amb força detall el seu encaix en aquests entramat legislatiu tot fent remissions, derogacions i modificacions[70] - compartint, com veurem, organismes de control i d'execució-. Tot i això, s'han assenyalat mancances en aquesta regulació. I fins i tot s'ha dit que el Reglament era innecessari ja que per assolir els seus objectius basta amb la modificació de les lleis vigents. És difícil compartir aquestes crítiques; especialment la segona, que menysté la necessitat d'una regulació amb una perspectiva global i unitària d'un fenomen d'abast i transcendència global.

VI.3 *Obligacions dels proveïdors, usuaris, representants autoritzats, importadors, distribuïdors i fabricants*

El Reglament regula amb minuciositat les obligacions específiques de totes i cadascuna de les persones físiques i jurídiques que participen en la que qualifica com a "complexa cadena de valor de la IA"[71]. Consisteixen essencialment en donar compliment als requisits exigits als sistemes de risc alt.

Els principals obligats són els proveïdors, definits com a les persones físiques o jurídiques, autoritats públiques, agències o organismes, que hagi desenvolupat o per a les quals s' hagi desenvolupat un sistema d'IA amb l'objectiu d'introduir-lo en el mercat o per posar-lo en servei sota el seu nom o marca comercial. Quan el sistema es un component de seguretat d'un producte, l'obligat de complir les obligacions com a proveïdor és el fabricant de l'aparell. Assumeixen també les obligacions dels proveïdors els distribuïdors, importadors, usuaris o tercers que modifiquin de manera substancial

[67] Juli Ponce, "Reserva de humanidad y supervisión humana de la IA" a El Cronista, numero 100, 2022, pag. 58-67.

[68] Concretament, obliga, entre altres, a incorporar copies de seguretat, determinades especificacions en les instruccions d'us, mecanismes de esmenar biaixos en el cas de sistemes que continuen aprenent i "mesures" per prevenir ciber-atacs. La UE està elaborant uns proposta de Reglament UE sobre ciber-seguretat.

[69] Com els Reglaments recents sobre la Seguretat de productes Digitals o la de Serveis Digitals o els que protegeixen drets i interessos com els drets de privacitat, de no discriminació, d'autor, de propietat intel·lectual, dels consumidors, a la competència, amb les corresponents vies de reclamació i de recurs jurisdiccional.

[70] Vegeu els arts. 75 a 82.

[71] Considerant 60.

un sistema de risc alt ja introduït en el mercat o posat en servei o en modifiquin la finalitat prevista. Els proveïdors podran demostrar que compleixen les obligacions mostrant que els sistemes són conformes amb normes harmonitzades o amb les "especificacions comunes" que la Comissió està obligada a establir en els àmbits en els quals no existeixin normes harmonitzades[72].

En segon lloc s'imposen obligacions rellevants, com a "usuaris" de sistemes de risc alt, a tota persona física o jurídica, autoritat pública, agència o organisme (inclosos els de la UE) que utilitzi un sistema d'IA "sota la seva pròpia autoritat", llevat que l'ús "s'emmarqui en una activitat personal de caràcter no professional"[73].

Finalment, també s'imposen obligacions als importadors, distribuïdors i, fins i tot, a tercers, com ara els venedors i subministradors de software o els proveïdors de serveis a la xarxa. Cal destacar que a banda de les obligacions específiques de cadascun dels obligats, tots ells tenen l'obligació de comprovar que la resta dels partícips en la cadena de valor han complert les seves obligacions[74].

VI.4 *Avaluació de la conformitat dels sistemes*

Es preveu encara un darrer requisit, que per la seva importància mereix dos llargs capítols a part: l'avaluació de la conformitat a la qual s'han de sotmetre tots els sistemes d'alt risc abans de l'entrada en el mercat o la posada en servei, per tal de comprovar que compleixen els requisits exigits pel Reglament. Amb tot, per evitar duplicitats, càrregues excessives als operadors o per facilitar transitòriament l'aplicació del Reglament, es preveuen importants modulacions i presumpcions de la conformitat.

Així, en el cas dels sistemes incorporats a robots i drons i regulats actualment en normes harmonitzades que estableixen requisits similars als del Reglament, els proveïdors podran optar per un control intern sota la seva responsabilitat enlloc del control extern realitzat per organismes notificats[75]. En la resta de sistemes, és a dir els "independents", "en la fase inicial d'aplicació del Reglament" (sic) el control serà sempre intern, amb la única excepció dels sistemes d'identificació biomètrica remota no prohibits, respecte

[72] Vegeu els arts. 40 i 41.

[73] La C.C, a partir del fet que els usuaris desenvolupen un paper important en la protecció de drets, valors, salut i seguretat, proposa reforçar les seves obligacions -i funcions- en detriment de les dels proveïdors. Com obligacions dels usuaris s'afegeix la designació de persones competents responsables de la supervisió humana dels sistemes o la notificació d'incidències i de mal funcionament. Quan el usuaris són autoritats públiques s'hi afegeix el registre d'usos en el registre de la base de dades de la Unió i la obligació de donar informació a les persones físiques objecte de la utilització de sistemes de risc alt.

[74] Començant pels proveïdors que, quan consideren que un sistema que han fet entrar en el mercat o han posat en funcionament ha deixat de ser conforme amb el Reglament, ho han de notificar als distribuïdors i adoptar les mesures necessàries per adequar-lo o retirar-lo del mercat (art. 21).

[75] En aquests casos només calen noves avaluacions respecte dels requisits del Reglament no coberts per la legislació harmonitzada o quan es produeixin canvis en la finalitat del sistema o en els algoritmes predeterminats.

dels quals l'avaluació serà externa -llevat que el proveïdor demostri que ha aplicat normes harmonitzades-.

L'avaluació externa la faran els denominats "organismes notificats", que seran designats i homologats per l'autoritat nacional de supervisió de la IA, que cada estat ha de crear. Es regula amb detall: els requisits que han de complir els organismes notificats -per tal de garantir-ne la competència tècnica, la independència i la imparcialitat-; el procediment d'homologació; l'obligació de notificar-la a la Comissió i a la resta d'Estats membres -que poden oposar-s'hi-; el procediment d'avaluació i els actes posteriors a l'avaluació - "declaració UE de conformitat", certificacions, marcatge de la conformitat dels sistemes-; la conservació de documents; i la inscripció en el registre i en la base de dades de la UE.

Es preveu que, en determinats supòsits, puguin actuar com a organismes notificats les autoritats encarregades de l'aplicació de la legislació penal, de la d'immigració i asil, així com determinats organismes i agències de la Unió i les autoritats estatals de vigilància d'altres mercats [76].

En tot cas, s'obliga la Comissió Europea a anar adaptant la regulació d'aquest requisit mitjançant actes de delegació.

Finalment es preveu encara una important exempció de l'avaluació quan "qualsevol autoritat de vigilància del mercat" de qualsevol Estat membre de la Unió consideri que ho requereix la seguretat pública, la protecció de la vida i la salut, el medi ambient o "els actius de les industries i infraestructures". La decisió se sotmet a un seguit de condicions que intenten acotar l'abast d'aquesta previsió certament perillosa[77]. La C.C. proposa la supressió d'aquesta exempció, mentre que el Consell afegeix un nou supòsit d' exempció en casos d'urgència i de perill per a la vida o la seguretat física de les persones[78].

VII. MESURES DE SUPORT A LA INNOVACIÓ

Com s'ha exposat a l'inici, el suport a la IA es produeix en la Proposta mitjançant les normes harmonitzades que acabem d'analitzar, que fomenten "la unitat del mercat intern europeu de la IA". Tanmateix a aquestes normes s'hi afegeix una mesura específica de suport a la innovació consistent en la creació d'uns "espais controlats de proves", que han d'establir els Estats o el Supervisor Europeo de Protecció de Dades

[76] És el cas de les autoritats de vigilància dels mercats previstes a la legislació europea sobre seguretat de productes; de les autoritats nacionals de supervisió dels serveis financers; de les encarregades de "l'aplicació de la legislació penal" o de les competents en matèria d'asil i immigració o de les encarregades de la Protecció de Dades.

[77] P.e. l'autorització té un període de vigència limitat; cal informar la Comissió i als altres Estats membres de la decisió. Ambdós tenen 15 dies per formular objeccions. La Comissió adopta la decisió final.

[78] La podrien acordar les autoritats encarregades de l'orde públic o de protecció civil.

amb l'objectiu de facilitar el desenvolupament, la prova i la validació de sistemes qualificats com a "sistemes innovadors", abans que entrin en el mercat i sota la supervisió de les autoritats competents.

La regulació d'aquesta única, i possiblement minsa mesura, es caracteritza: a) per la voluntat de potenciar la dimensió europea d'aquest mecanisme de suport[79]; b) la voluntat d'ampliar al màxim el tipus de dades personals que es poden emprar en les proves, tot establint però garanties per tal d'evitar usos indeguts[80] i c) la previsió de mesures de suport als proveïdors i usuaris de "petita escala" [81]. El Consell proposa una regulació molt extensa de les proves -que preveu tant dins com fora dels espais de controlats-, i dona un relleu especial a totes les mesures de suport, en particular a les adreçades a les "pimes" i "microempreses".

VIII. GOVERNANÇA

Sota la rúbrica de Governança es regula la qüestió cabdal de les autoritats que han de garantir l'execució i, més concretament, l'aplicació efectiva i uniforme del Reglament arreu del territori de la Unió.

Tot i que, com és propi de l'UE, l'execució del Reglament en principi hauria de correspondre en gran mesura als organismes corresponents dels Estats, la Proposta atribueix a la Comissió un protagonisme executiu destacat a fi de garantir la uniformitat interpretativa i executiva, i la cooperació entre Estats i d'aquests amb l'UE.

Amb aquest objectiu es crea un "**Comitè Europeu d'IA**", format per les autoritats nacionals de supervisió de cada Estat i el Supervisor Europeu de Protecció de Dades. El presideix la Comissió, i en convoca les reunions, estableix l'ordre del dia i li dona suport administratiu i "analític" (sic). A les reunions s'hi poden convocar experts i observadors. El Comitè, té atribuïda la funció d'assessorar i assistir la Comissió i té com a finalitats les de contribuir a coordinar les autoritats nacionals i la Comissió, "les orientacions i els

[79] Així p.e. els espais controlats han de garantir el compliment no solament del Reglament sinó també de la resta de la legislació de la Unió i dels Estats membres; les autoritats nacionals que hagin establert espais controlats coordinaran les seves activitats i cooperaran en el marc del Comitè Europeu d'IA -amb informes adreçats al Comitè i a la Comissió sobre resultats. S'atribueix a la Comissió la regulació, mitjançant actes d'execució, de les modalitats, condicions de funcionament, criteris d'admissibilitat, drets i obligacions dels participants i de procediments de sol·licitud, selecció i participació en l'espai .

[80] P.e. es permet la utilització de dades recopilades legalment però per altres finalitats -fins i tot dades sense anonimitzar-, quan ho requereixi l'aplicació de la "legislació penal", la prevenció d'amenaces a la seguretat pública, la salut pública o la protecció de medi ambient. Es preveu, però, que els participants respondran de qualsevol perjudici causat a tercers, és limitarà l'accés a les dades a determinades persones i s'eliminaran les dades en cloure´s el "control".

[81] Obligant els Estats a promoure un accés prioritari als espais controlats de proves; a organitzar activitats sobre l'aplicació del Reglament; a establir un canal de comunicació amb proveïdors i usuaris de petita escala i "agents innovadors"; a banda de tenir en compte els seus interessos i necessitats en fixar taxes.

anàlisis" de la Comissió i de les autoritats nacionals de supervisió, i a garantir "l'aplicació coherent" del Reglament[82] .

La C.C. ha presentat un conjunt d'esmenes molt interessant adreçada a crear una potent, i poc freqüent, "Execució a escala europea", s'aplicarà als "problemes que afecten diversos Estats membres" amb l'objectiu de "contribuir a l'aplicació uniforme del Reglament, i a reforçar el mercat únic digital". La Comissió Europea tindria un paper determinant en aquesta "execució" [83], a banda de convertir-se en una "autoritat de vigilància del mercat". El Consell, amb el mateix objectiu de reforçament, fa un llistat obert d'àmbits en els quals la Comissió haurà de dictar directrius sobre "l'aplicació pràctica" del Reglament.

En relació al Comitè Europeu d'IA la C.C. proposa incrementar substancialment les seves competències[84] per tal de potenciar la seva contribució a l'aplicació uniforme del Reglament i l'assessorament i assistència a la Comissió; ultra reforçar la seva independència[85]. També vol potenciar-lo com a "fòrum d'intercanvi" entre autoritats nacionals de supervisió, com a instància d'arbitratge de litigis entre autoritats i entre Estats i com a lloc de trobada de la industria, les empreses emergents, les "pimes", la societat civil i el mon acadèmic[86]. També prosa canvis rellevants pel que fa a: a) la composició del Comitè -que estaria format exclusivament per un representant de cada Estat-, b) el funcionament intern -que regula amb cert detall i dona les pautes que hauria l'elaboració del futur reglament intern- i c) les funcions -que amplia i precisa-. Preveu a més la creació d'un potent Grup central d'experts independents, de suport a la Comissió i a les autoritats de vigilància del mercat.

Pel que fa a la Governança que correspon als Estats, l'organisme clau és l'autoritat nacional de supervisió de la IA, la qual, a més de designar i homologar els organismes

[82] A tals efectes, el Comitè recopila i comparteix coneixements tècnics i bones pràctiques entre els Estats; contribueix a la uniformització de les pràctiques administratives i emet dictàmens, recomanacions o contribucions escrites.

[83] Vegeu l'Exposició de Motius del "Projecte d'Informe" de la C.C. i les nombres competències que se li atorguen en els esmenes 259 a 270. Concretament se li reconeixerien d incoació de procediments contra sistemes d'IA per infracció del Reglament; "poders d'investigació i execució"; competències de cooperació i intercanvi d'informació amb les autoritats nacionals; competències per sol·licitar informació; "poders" per realitzar entrevistes i prendre declaracions; "poders" d'inspecció; competències per decidir l'incompliment de les obligacions dels operadors; adopció de mesures provisionals i publicació de les decisions; competències per sol·licitar informació, per realitzar entrevistes i prendre declaracions; competències d'inspecció; competències en cas d'incompliment dels operadors de les obligacions respectives; adopció de mesures provisionals en cas de decisions d'incompliment i d'ordenar la publicació de les decisions corresponents.

[84] Esmenes 199 a 211.

[85] En relació a la seva estructura, funcionament, elecció del president i vicepresident, convocatòria de reunions i fixació de l' ordre del dia (vegeu esmenes 185 a 198).

[86] Finalment, a banda del Comitè Europeu, el Reglament també crea un nou Comitè, que s'afegeix als més de 300 comitès del Reglament UE 182/2011, i que assistirà la Comissió en l'adopció dels actes delegats que li atribueix el Reglament IA.. Aquest Comitè, com en tots els comitès que s'integren en la denominada comitologia, està integrat per un representant de cada Estat, i pot formular objeccions i fins i tot revocar la delegació.

notificats i de fer el seguiment de llur activitat, actua com a autoritat de vigilància del mercat i té competències rellevants tant en el procés de seguiment posterior a la comercialització dels sistemes com en l'avaluació dels riscos que generin i en l'adopció de les mesures correctores pertinents. Aquestes autoritats són organismes independents, creats pels Estats respectius[87], als quals han de dotar de personal tècnic qualificat i de recursos suficients. Els Estats han d'informar anualment la Comissió sobre aquests recursos[88]. Les autoritats nacionals d'IA estaran en contacte permanent entre elles. Finalment, cal recordar, que per tal d'evitar duplicitats, el Reglament preveu un seguit de supòsits en els quals les funcions d'autoritat nacional de vigilància del mercat d'IA s'atribueixen a autoritats de vigilància d'altres mercats previstes en altres disposicions de la UE[89].

IX. SEGUIMENT POSTERIOR A LA COMERCIALITZACIÓ, PROCEDIMENTS PER AVALUAR ELS RISCOS I MESURES CORRECTORES

Pel que fa al seguiment, els proveïdors han d'establir, d'acord amb un model que aprovarà la Comissió, "un sistema i un pla" adequats a la tecnologia emprada i als riscos previsibles. Han de notificar a les autoritats de vigilància del mercat qualsevol incidència greu que pugui afectar drets fonamentals i aquestes n'informaran als organismes nacionals encarregats de la protecció dels drets fonamentals de la UE[90].

Les autoritats de vigilància del mercat tenen ampli accés a les dades, la documentació, les dades d'entrenament, validació i prova emprats pel proveïdor i, "en cas necessari i prèvia sol·licitud motivada", als "codi font" o fitxers d'instruccions escrites que fan "funcionar" els programes. L'accés al codi font sol plantejar problemes i en cas de conflicte les empreses que els dissenyen i desenvolupen solen al·legar, amb èxit, drets relacionats amb la llibertat de creació, la propietat intel·lectual i fins i tot la protecció de la privacitat de tercers, per tal d'evitar l'accés al codi. El Consell proposa que només es pugui accedir al codi dels sistemes independents que afecten drets fonamentals i tan

[87] Els Estats poden designar més d'una autoritat de supervisió (potser pensant en els estats federals o descentralitzats?) -però en aquest cas ho ha de motivar davant la Comissió. L'autoritat que supervisa l'aplicació del Reglament per part de les institucions, agències i organismes de la UE és el Supervisor Europeu de Protecció de Dades. L'Estat espanyol, avançant-se als altres Estats, ha creat ja l'Agència Espanyola de Supervisió de la IA, amb seu a A Coruña.

[88] Els Estats han de presentar a la Comissió un informe anual sobre els recursos esmerçats i una avaluació de la seva idoneïtat. La Comissió els transmet al Comitè Europeu pel seu debat i formulació de possibles recomanacions. La Comissió facilitarà l'intercanvi d'experiències entre autoritats nacionals. La C.C. presenta una esmena adreçada a declarar i garantir el caràcter independent de les autoritats nacionals de supervisió.

[89] Vegeu la nota 76.

[90] La Comissió elaborarà "les orientacions específiques" per facilitar el compliment de les obligacions dels proveïdors relatives a la notificació de les referides incidències (art. 62.2).

sols quan hagin sigut insuficients altres procediments per obtenir la informació requerida.

Com a instrument per facilitar el seguiment del compliment dels requisits, la Comissió, amb la col·laboració dels Estats, crearà i mantindrà una "Base de Dades de la UE per sistemes de risc alt independents", que es nodrirà de les dades que hauran de lliurar-li els proveïdors. Les dades seran accessibles al públic. Tanmateix la informació que contindrà té un relleu força limitat[91].

En relació a l'avaluació dels riscos produïts i a les mesures per corregir-los, el Reglament distingeix el procediment aplicable als riscos "a nivell nacional", el de "salvaguarda de la Unió" i el dels riscos que no assoleixin aquestes dimensions territorials.

En el primer supòsit, com ja he apuntat, s'atribueix a l'autoritat nacional de vigilància del mercat la competència per: a) determinar si un sistema presenta riscos per a la salut, la seguretat o els drets fonamentals, b) avaluar el compliment dels requisits i obligacions que l'imposa el Reglament i c) exigir a l'operador l'adopció de les mesures correctores oportunes o la retirada del mercat. Ha d'informar l'organisme estatal de protecció dels drets fonamentals i a l'organisme notificat corresponent. Si es considera que el risc pot afectar d'altres Estats de la Unió, informarà la Comissió i els Estats dels riscos i les mesures adoptades. Indicarà si el problema és conseqüència d'un incompliment de requisits o d'una deficiència de les normes harmonitzades. Després de 3 mesos sense objeccions per part de la Comissió o dels Estats, la mesura adoptada per l'Estat es considerarà justificada.

Si dins d'aquest termini un Estat formula alguna objecció, o la Comissió considera que la mesura adoptada es contrària al Dret de la Unió, es posa en marxa el procediment de salvaguarda de la Unió: la Comissió, prèvia consulta amb l'Estat membre i els operadors afectats, avalua la mesura adoptada; si es considera justificada, tots els Estats l'adoptaran, si és injustificada, serà retirada. Si la causa de la deficiència és la normativa UE, es modificarà[92].

Finalment, interessa destacar que la Proposta (art. 84.2), ultra la ja citada exigència d'avaluar anualment la necessitat de modificar la llista dels sistemes de risc alt, preveu un "**sistema d'avaluació i revisió permanent"** de l'aplicació del Reglament que obliga la

[91] Vegeu l'art.60.4

[92] En el cas que les avaluacions mostrin que un sistema és conforme amb el Reglament però una autoritat de vigilància del mercat comprovi que presenta un risc per a la salut, la seguretat, els drets fonamentals, el compliment de les obligacions en virtut del Dret la Unió o per a la protecció de l'interès públic, demanarà al proveïdor la adopció de mesures correctores, abans entrada mercat, o la retirada del mercat, si ja hi ha entrat. L'Estat n'informarà la Comissió i els altres Estats. La Comissió consultarà els proveïdors i els altres Estats, avaluarà les mesures adoptades per l'Estat i els resultats de la consulta, i adoptarà la decisió que correspongui i la comunicarà a tots els Estats.

Comissió a presentar cada 4 anys al Parlament i al Consell un informe, que es farà públic, sobre aquesta aplicació i sobre l'eficàcia dels Codis de conducta voluntaris[93].

X. VIES DE RECLAMACIÓ I RECURS JURISDICCIONALS

Com ha observat críticament un sector de la doctrina des de l'inici, la Proposta pràcticament no incorpora vies de reclamació ni de recurs jurisdiccional[94]. Tant el Consell com sobretot la C.C. es fan ressò d'aquesta crítica. Concretament la C.C proposa un nou i important Capítol en el qual es reconeix el dret de les persones físiques i grups de persones físiques a presentar, davant l'autoritat nacional de supervisió, reclamacions contra els proveïdors o usuaris d'un sistema d'IA, quan considerin que han vulnerat "la seva salut, la seva seguretat o els seus drets"[95]. L'autoritat nacional de supervisió ha de resoldre abans dels 6 mesos de la presentació de la reclamació que ha adoptat la decisió recorreguda.

Pel que fa als recursos, es limita a reconeix a les persones físiques i jurídiques el "dret a la tutela judicial efectiva contra una decisió jurídicament vinculant d'una autoritat nacional de supervisió que les afecti". Les accions s'exerceixen davant els tribunals del Estat membre en el qual estigui establerta l'autoritat nacional de supervisió.

XI. CONFIDENCIALITAT

El Reglament imposa un deure de confidencialitat a les autoritats nacionals competents i els organismes notificats sobre la informació i les dades obtingudes en exercici de les seves funcions[96]

XII. SANCIONS

[93] La C.C. presenta també esmenes adreçades a reforçar la participació de les persones interessades i organitzacions de la societat civil en l'actualització de la llista de sistemes de risc alt, així com en les activitats del Comitè i els espais de proves, entre altres.

[94] Es limita a delegar en els Estats l'establiment d'un recurs contra les decisions dels organismes notificats (art. 45). Certament, com he assenyalat abans, la legislació europea i les legislacions estatals de de protecció de dades, de drets de privacitat, de protecció de drets de propietat intel·lectual, dels consumidors, drets d'autor preveuen vies de reclamació i recursos jurisdiccionals que permeten la defensa de drets i interessos en front vulneracions causades per sistemes d'IA, però no cobreixen de manera general i específica els drets i interessos protegits pel Reglament d'IA.

[95] I se'ls hi reconeix explícitament el dret a ser escoltats en el procediment de tramitació de la reclamació.

[96] Amb l'objectiu de protegir "en particular": els drets de propietat intel·lectual, la informació empresarial confidencial o els secrets comercials, inclòs el codi font; l'aplicació eficaç del Reglament a efectes d'inspeccions i investigacions; els interessos públics i de seguretat nacional; i la "integritat" de les causes penals o els procediments administratius (art. 70.1).

Correspon als Estats establir **el règim sancionador** i els organismes, jurisdiccionals o no, que l'han d'aplicar, i comunicar-los a la Comissió. La C.C. proposa que també la Comissió Europea pugui imposar multes. El Reglament es limita: a exigir que les sancions siguin "efectives, proporcionades i dissuasives"; a tipificar les conductes que poden ser objecte de multes administratives; a establir el topall màxim -per cert força elevat- que poden assolir les quanties de les multes en cada tipus d'infracció[97]; i a assenyalar les circumstàncies que han de tenir en compte els Estats a la hora de fixar les quanties esmentades[98].

Es deixa a la decisió dels Estats la possibilitat d'imposar multes administratives a les seves autoritats i organismes públics. Les multes administratives a institucions, agències i organismes de la Unió les imposa el Supervisor Europeu de Protecció de Dades.

XIII. ENTRADA EN VIGOR I APLICACIÓ

Com he apuntat abans, l'entrada en vigor del Reglament es produirà als 20 dies després de la publicació, i l'aplicació als 24 mesos a partir entrada en vigor, llevat la de la legislació europea relativa a l'espai de llibertat, seguretat i justícia respecte de la qual el termini serà de 36 mesos. El Consell proposa que aquest termini 36 mesos s'apliqui amb caràcter general. A la hora de valorar aquesta regulació cal tenir en compte, d'una banda, el temps que és necessari per tenir realment operatius els organismes europeus i estatal de governança i d'execució del Reglament i, per altra banda, la urgència d'evitar al màxim l'aplicació sense límits de sistemes que generin riscos a la salut, la seguretat i els drets fonamentals. Des d'aquesta doble perspectiva la diferenciació entre entrada en vigor i aplicació es pot considerar adequada mentre que els terminis superiors als 24 mesos es poden considerar excessius. I, en tot cas, siguin quins siguin els terminis d'aplicació que finalment s'estableixin, caldrà interpretar i aplicar "extensivament" el concepte de "canvi significatiu" de l'art. 83.2 per tal de minimitzar els riscos que poden provocar els sistemes introduïts en el mercat abans de la data d'inici de l'aplicació del Reglament.

XIV. CODA

[97] Així, p.e., l'incompliment de la prohibició de les pràctiques d'IA o dels requisits dels sistemes que utilitzen dades d'entrenament, se'ls hi apliquen multes administratives de fins a 30 milions d'euros o, si l'infractor és una empresa, fins el 6% del volum del negoci total anual mundial de l'exercici financer anterior si aquesta quantia fos superior als 30 milions. Per a la resta d'incompliments dels requisits, les multes poden ser de màxim de 20 milions o el 4% volum de negoci. I de 10 milions o el 2% si la infracció consisteix en la presentació d'informació, inexacta, incompleta o enganyosa.

[98] Per exemple la naturalesa, gravetat i duració de la infracció, la reincidència o el volum i la quota de mercat de l'operador.

Per poder fer una valoració definitiva del Reglament, tant des del punt de vista jurídic com del de la capacitat real de limitar els riscos que generen els sistemes d'IA, caldrà esperar al final del procés legislatiu i la seva interpretació i aplicació. Caldrà esperar per tal de poder comprovar si és suficient per garantir la salut, la seguretat i els drets fonamentals de la Unió i per assegurar l'autonomia i la dignitat de les persones i la prevalença de la intel·ligència humana sobre la IA.

En aquest moment, de la Proposta en destacaria: la seva necessitat i fins i tot urgència; el rigor i la participació extraordinària en qualitat i quantitat, produïda al llarg de tot el procediment legislatiu i en l'etapa preliminar; la decisió de regular l'IA des de valors ètics i de principis polítics demo-liberals; la cerca de l'equilibri entre drets i bens, en potencial tensió, protegits tots ells pel Dret de la Unió; l'estratègia de basar els límits jurídics en el criteri de risc; el reforç de les facultats executives de la Comissió per tal de garantir la uniformitat interpretativa i executiva del Reglament; i l'establiment de mecanismes que han de permetre l'adaptació permanent del Reglament als canvis de la IA i als avenços que sorgeixin del debat ètic i filosòfic en aquest àmbit.