L’Europa futura, meno diritti per più competitività

Nel suo rapporto Draghi dice che non possiamo avere una forte tutela dei diritti fondamentali e allo stesso tempo aspettarci di promuovere l’innovazione. La critica è rivolta in particolare al GDPR, che protegge i nostri dati personali. Ma è una critica senza fondamento.

Maurizio Borghi

Tra le cause della scarsa competitività delle imprese europee nei settori avanzati dell’informatica, oggi chiamata “intelligenza artificiale”, il rapporto Draghi individua la regolamentazione dell’Unione Europea sull’uso dei dati[1]. Considerata troppo complessa e onerosa rispetto ai sistemi in vigore nei principali paesi leader, come USA e Cina, tale regolamentazione penalizzerebbe i ricercatori e gli innovatori europei impegnati nella competizione globale.

Una settimana dopo la presentazione del rapporto Draghi, una lettera aperta firmata da circa quaranta CEO di aziende (europee e non), pubblicata sui principali organi di informazione, rilanciava l’allarme: la mancanza di “certezza normativa” sull’utilizzo dei dati rischia di condannare l’Europa a rimanere “ulteriormente indietro” nella corsa all’intelligenza artificiale, mettendo a repentaglio un futuro promettente di crescita e prosperità.

Sebbene si parli di “normativa UE” in generale, il colpevole sembra però essere uno solo: il Regolamento generale sulla protezione dei dati personali, meglio noto come GDPR[2]. A pag. 79 del rapporto Draghi leggiamo che

1 EU competitiveness: Looking ahead. Tutte le citazioni in questo articolo si riferiscono al documento *The future of European competitiveness – Part B: In-depth analysis and recommendation*, 9 September 2024.

2 Il GDPR (General Data Protection Regulation) è il regolamento n. 2016/679 dell’Unione europea che stabilisce le norme per il trattamento dei dati personali dei cittadini dell’Ue.

esiste un rischio di “overlaps and inconsistencies” tra i principali ordinamenti sull’impiego dei dati, ma nel resto del rapporto si nomina unicamente il GDPR e solo sporadicamente, e senza avanzare particolari rilievi, gli altri regolamenti Ue come il Data Act, il Data Governance Act e soprattutto il recente Artificial Intelligence (AI) Act. Il nocciolo del problema è espresso candidamente nei termini seguenti:

As in global AI competition ‘winner takes most’ dynamics are already prevailing, the EU faces now an unavoidable trade-off between stronger ex ante regulatory safeguards for fundamental rights and product safety, and more regulatory light-handed rules to promote EU investment and innovation, e.g. through sandboxing, without lowering consumer standards (p. 79).

Il senso è chiaro: non possiamo avere una forte tutela dei diritti fondamentali e allo stesso tempo aspettarci di promuovere l’innovazione. Il *trade-off* è inevitabile, e prepariamoci ad affrontarlo.

Ma quali sarebbero gli ostacoli che questa “strong ex ante regulatory safeguard” pone all’innovazione e alla competitività delle imprese europee? Il rapporto Draghi ne individua tre: i) il GDPR impone oneri alle imprese europee impegnate nei settori di punta dell’intelligenza artificiale che le penalizzano rispetto ai concorrenti USA e cinesi; ii) l’applicazione frammentaria e incoerente del GDPR crea incertezza sull’uso legittimo dei dati e iii) questa incertezza impedisce, in modo particolare, l’uso efficiente dei dati sanitari per lo sviluppo di strumenti di intelligenza artificiale nel settore medico e farmaceutico.

Verifichiamo se gli argomenti a sostegno di queste tesi possono reggere a un’analisi un po’ approfondita.

Primo argomento: alti costi di compliance

Sul primo punto – gli oneri imposti dal GDPR alle imprese europee – il rapporto cita alcuni numeri:

Estimates point to high GDPR compliance costs, up to EUR 500,000 for SMEs and up to EUR 10 million for large organisations. Furthermore, due to these compliance costs, EU companies decreased data storage by 26%

and data processing by 15% in relation to comparable US companies. (p. 319)

Le fonti riportate in nota sono: due prospetti informativi di società di consulenza (PCH e Veritas), un articolo del Financial Times e, quale unico lavoro scientifico, un working paper di un noto think tank statunitense. Nel paper viene presentato uno studio empirico, basato su questionari distribuiti a società statunitensi ed europee, che fornisce alcune stime dell'impatto del GDPR sui costi di produzione in diversi settori dell'economia, digitale e non. Senza entrare qui nel merito di questo lavoro, e di altri di simile tenore non citati nel rapporto Draghi[3], vale la pena di fare tre osservazioni. Innanzitutto, è un errore metodologico presentare il GDPR come un onere che grava sulle imprese europee. Si tratta infatti, com'è noto, di un regolamento che si applica allo stesso modo a tutte le imprese, europee e non, che trattino dati personali di cittadini dell'Unione. È perfettamente lecito mettere a confronto i costi delle imprese soggette al GDPR (ovvero quelle che trattano dati dei cittadini Ue) con quelli di chi non vi è soggetto (tutte le altre); dobbiamo però avvertire che il confronto non è tra "imprese europee" e "imprese non-europee", bensì tra soggetti che, indipendentemente dalla loro sede legale, trattano o non trattano dati Ue e che pertanto, molto verosimilmente, operano su mercati diversi e quindi non sono in competizione tra di loro[4]. Rappresentare il GDPR come un costo che mina la competitività delle imprese europee è una forzatura: se di costo si tratta, esso incide in eguale misura su tutte le imprese che competono sul mercato unico europeo.

Va poi aggiunto che è inevitabile, e persino scontato, che la competizione su mercati regolati comporta dei costi di *compliance*. Ma è questa una ragione sufficiente per preferire mercati senza regole? Anche a prescindere dalla tutela di diritti fondamentali, primi fra tutti i diritti dei lavoratori e dei cittadini, un'analisi d'impatto che si rispetti dovrebbe considerare non solo i costi, ma anche i benefici derivanti dall'operare in un mercato soggetto a regole e standard comuni. Infatti, se la GDPR-compliance comporta senz'altro dei

3 Per una critica delle metodologie impiegate negli studi *industry-sponsored* sui costi del GDPR si veda CNIL, The economic impact of GDPR, 5 years on (24 April 2024).

4 La competizione tra imprese con costi di *compliance* differenti si verifica unicamente quando un'azienda sviluppa un prodotto o servizio utilizzando esclusivamente dati personali provenienti da fuori dell'Ue e lo introduce successivamente nel mercato Ue (o viceversa). Ma si tratta di una situazione particolare che non rappresenta certo la norma.

costi per le imprese, permette anche loro di valersi della libera circolazione di dati personali all'interno di un vastissimo mercato unico regolato[5]. Le stesse aziende che oggi si lamentano dei limiti imposti dal GDPR all'utilizzo dei dati per addestrare le loro intelligenze artificiali, hanno in realtà beneficiato per anni della possibilità di raccogliere massicciamente dati personali in tutto il mercato unico proprio grazie al GDPR. Del resto, se il GDPR fosse unicamente una zavorra per l'innovazione, non si spiegherebbe perché la Cina abbia scelto di adottare uno strumento regolativo che ne ricalca da vicino i principi e il funzionamento.

Non sorprende che i benefici della regolazione non emergano da studi empirici principalmente orientati a rilevare il punto di vista delle imprese. Ma l'uso selettivo delle fonti per evidenziare unilateralmente i costi, dimenticandosi i vantaggi, denota una prospettiva quantomeno parziale, che non si accorda con una rappresentazione obiettiva del mercato.

Secondo argomento: incertezza sull'uso legittimo dei dati

Veniamo qui al secondo fattore di criticità individuato dal rapporto Draghi, ovvero l'applicazione incoerente del GDPR tra gli Stati membri, quale fonte di incertezza per le imprese. Il punto è anche al centro della lettera aperta dei CEO aziendali: "negli ultimi tempi – si legge nella lettera – le decisioni normative sono diventate frammentate e imprevedibili, mentre gli interventi delle autorità europee per la protezione dei dati hanno creato una grande incertezza sul tipo di dati che possono essere utilizzati per addestrare i modelli IA". Non è specificato quali siano le leggi "imprevedibili" emanate "negli ultimi tempi", e perché le autorità garanti avrebbero creato una "grande incertezza". In realtà, le autorità garanti qualche contributo alla certezza lo hanno fornito: il rapporto della task force EDPB su ChatGPT – giusto per fare un esempio – chiarisce in modo preciso quali sono le condizioni per un legittimo uso dei dati personali a scopo di training di IA generativa. E poi, siamo davvero certi che l'innovazione sia impossibile senza certezze assolute sull'uso legittimo dei dati? Negli USA, la ben maggiore incertezza riguardo alla qualificazione dell'uso di opere protette da copyright come fair use non sembra aver ostacolato lo sviluppo vertiginoso dei modelli di IA generativa.

5 Il terzo del mondo per numero di abitanti, dopo India e Cina ma prima di USA.

Il rapporto Draghi fornisce però qualche indicazione in più. Riprendendo i lavori della Commissione illustrati in una comunicazione del 2020, il rapporto individua la principale fonte di incertezza nel fatto che il GDPR richiede agli Stati membri di legiferare in alcuni ambiti di applicazione del regolamento: ciò condurrebbe al noto fenomeno del *gold-plating*, per cui alcuni Stati membri approfittano della discrezionalità lasciata dalla normativa europea per introdurre leggi nazionali che eccedono quanto richiesto dalla normativa. Il risultato è, appunto, una frammentazione tra le norme in vigore nei diversi stati membri.

In verità, le criticità riscontrate dalla Commissione nel working document che accompagna la comunicazione del 2020, non riguardano solo fenomeni di gold-plating, ma anche l'esatto opposto, ossia il fatto che alcuni Stati membri restringono eccessivamente i diritti delle persone senza specificare da quali obiettivi di interesse pubblico sarebbero giustificate tali restrizioni. Ma tra i punti sollevati dalla Commissione, il rapporto Draghi seleziona un solo esempio: la variazione dell'età del consenso tra alcuni stati membri:

As an example, divergence in the age of consent across Member States creates uncertainty in the application of data protection rights for children in the Single Market. (p. 319)

L'esempio può essere certamente indicativo di "incertezze" in alcuni settori dell'economia digitale (messaggistica, social networking, ecc.), ma appare tutt'altro che calzante nel contesto dell'uso dei dati personali per fini di addestramento dell'intelligenza artificiale. Se leggiamo le privacy policies delle principali aziende di IA generativa, la base legale che viene più comunemente dichiarata per l'utilizzo di dati personali ai fini di addestramento non è il consenso dell'interessato – difficile se non impossibile da ottenere per masse consistenti di dati – ma il legittimo interesse del titolare del trattamento dei dati[6]. Ora, delle due l'una: o il legittimo interesse non è una base legale sufficiente, e dunque i dati di milioni di cittadini europei vengono trattati illegalmente da queste imprese, oppure il consenso degli interessati non è necessario per quel tipo di utilizzo, e dunque la divergenza tra stati membri circa l'età del consenso è del tutto irrilevante[7]. In ogni caso, risulta forzato e un po' pretestuoso

6 Si veda tra tutte la privacy policy di OpenAI: https://openai.com/it/policies/eu-privacy-policy

7 Per determinare se sussiste un legittimo interesse al trattamento dei dati, è necessario considerare, nel bilanciamento tra gli interessi del titolare del trattamento e i diritti della

prendere questo esempio come paradigmatico delle "incertezze" capaci addirittura di compromettere la competitività delle imprese europee nei settori di punta dell'economia[8] digitale.

Terzo argomento: ostacoli agli usi secondari dei dati sanitari

Un rilievo più specifico avanzato dal rapporto Draghi riguarda l'uso secondario dei dati sanitari, quale "precondition for the further development of AI" (p. 196). Il rapporto ricorda che alcuni Stati membri già permettono l'uso secondario delle cartelle cliniche dei pazienti (in forma anonimizzata e in condizioni di sicurezza) per scopi di ricerca e sanità pubblica senza il consenso dell'interessato, ma lamenta il fatto che questa opzione non è stata recepita da tutti i paesi dell'Ue, generando così – ancora una volta – squilibri e incertezza. Senza dubbio, questo è un ambito in cui un intervento di armonizzazione potrebbe risultare vantaggioso e dare maggiore efficacia alla proposta di regolamento istitutivo dello spazio europeo dei dati[9].

Ma i dati sanitari non si esauriscono nelle cartelle cliniche dei pazienti, oggetto esclusivo di attenzione nel rapporto Draghi: includono un'ampia varietà di informazioni, sia personali che non, che riguardano diverse categorie di dati aggregati in forma anonima e in particolare quelli provenienti dalle sperimentazioni cliniche[10]. E gli usi secondari di questi dati non si riducono al training di sistemi di IA, ma comprendono la ricerca, il controllo pubblico sulle sperimentazioni, la replicabilità dei risultati, e molti altri ancora. Per questi usi secondari l'ostacolo non risiede nel GDPR o nella sua applicazione variabile tra gli Stati membri. Il vero problema è rappresentato dai soggetti privati (aziende farmaceutiche in primis) che detengono queste informazioni e, invocando un'interpretazione espansiva del segreto commerciale, si oppongono in tutte le sedi alla loro divulgazione o condivisione, anche quando prevista dai regolamenti. La Corte di giustizia

persona, anche se quest'ultima è un minore (Cons. 47 del GDPR). Ma questo vale indipendentemente dall'età del consenso stabilita per legge.

8 Ricordiamo che anche negli USA esistono divergenze significative tra le leggi dei singoli Stati federali circa l'uso dei dati dei minori.

9 Per una disamina seria e scientificamente fondata del problema si rimanda a Ugo Pagallo, *Il dovere alla salute. Sul rischio di sottoutilizzo dell'intelligenza artificiale in ambito sanitario* (Mimesis, 2022).

10 All'art. 33 della Proposta di regolamento sullo spazio europeo dei dati sono elencate ben 15 categorie di dati sanitari elettronici per l'uso secondario.

si è già pronunciata più volte su questo tema, censurando un'interpretazione espansiva del segreto commerciale che vanifichi gli obiettivi di interesse pubblico perseguiti dai regolamenti sull'accesso ai dati[11]. Per dare impulso all'uso secondario dei dati sanitari in senso ampio sarebbe dunque opportuna una revisione dei regolamenti che restringa l'ambito di applicazione delle disposizioni di "carve-out" a tutela del segreto commerciale, in linea con i pronunciamenti della Corte, riconoscendo pienamente i dati sanitari come un bene pubblico. Eppure, di raccomandazioni che vadano in questa direzione non c'è traccia nel rapporto Draghi, la cui sola preoccupazione è quella di agevolare l'uso delle cartelle cliniche dei pazienti da parte degli sviluppatori di modelli di IA.

Conclusioni: meno diritti uguale più competitività?

L'obiettivo di individuare i rimedi alla scarsa competitività delle imprese europee nei settori *data intensive* è lodevole. Peccato però che la corsa all'innovazione in questi settori stia diventando più che altro un pretesto per lanciare un attacco ai diritti fondamentali, avendo ben poco a che vedere con la rimozione di barriere all'innovazione e molto di più con l'ampliamento del controllo privato su beni pubblici come i dati[12]. L'assenza di "strong ex ante regulation" nei settori dell'information technology ha favorito in USA l'affermarsi di giganteschi monopoli che hanno compromesso irrimediabilmente il funzionamento del mercato, con buona pace della "competitività" delle imprese. L'esportazione in Europa del modello americano risponde principalmente ai desideri di questi monopolisti, che grazie al GDPR hanno già avuto accesso al mercato unico e raccolto masse di dati di cittadini europei,[13] di affermare la libertà di "fare quello che ci pare" con quei dati.

Vi sono almeno due ragioni per cui il *trade-off* draghiano tra forte tutela dei diritti fondamentali e sostegno all'innovazione è irricevibile. La prima è

11 Pari Pharma GmbH v EMA (T-235/15 | 2018), Amicus Therapeutics UK Ltd v EMA (T-33/17 | 2018), MSD Animal Health Innovation GmbH v EMA (C-178/18 P | 2022). Si veda anche la decisione dell'European Ombudsman in Cochrane Collaboration Research Group v EMA (Case 2650/2007/BEH).

12 Notiamo che tra i firmatari della lettera aperta figurano aziende in posizione dominante già più volte sanzionate per violazioni del GDPR e delle regole della concorrenza.

13 Spesso in violazione del GDPR stesso, come dimostra la lunga sfilza di sanzioni comminate a compagnie USA dalle autorità garanti degli stati membri.

che, come ha mostrato l'analisi qui svolta, si tratta di un'alternativa illusoria: non vi sono argomenti convincenti a sostegno dell'idea che, limando un po' il GDPR, la competitività delle imprese europee farebbe un balzo in avanti.

La seconda, più importante, è che i diritti fondamentali sono semplicemente materia non negoziabile. Si è spesso tentati di considerare la tutela della privacy e dei dati personali come diritti minori, sui quali è lecito e persino utile fare qualche compromesso. Occorre però ricordare che lo sviluppo della cosiddetta intelligenza artificiale non avviene nel vuoto, ma nel contesto del potenziamento di sistemi informatici destinati principalmente a compiti come la sorveglianza, la profilazione individuale, le decisioni algoritmiche e l'ottimizzazione predittiva, tutti ambiti che esercitano un impatto enorme sulle persone e sulla collettività nel suo insieme. L'applicazione del GDPR ha consentito alle autorità garanti, se non di prevenire almeno di sanzionare alcuni degli abusi più gravi nell'applicazione di questi sistemi. Tra questi, la sorveglianza dei dipendenti sui luoghi di lavoro, il monitoraggio dello "stato emotivo" dei clienti, l'uso di algoritmi opachi e discriminatori per determinare la concessione del credito o per assegnare carichi di lavoro ai propri dipendenti, il dossieraggio di milioni di cittadini per il riconoscimento facciale, il trasferimento illegale di dati personali al di fuori dell'Unione europea. Con la crescente diffusione di dispositivi che integrano questi (e molti altri) abusi, deregolamentare l'utilizzo dei dati personali ha un solo effetto certo: compromettere la tutela dei diritti fondamentali riconosciuti e garantiti dal diritto primario dell'Unione europea.