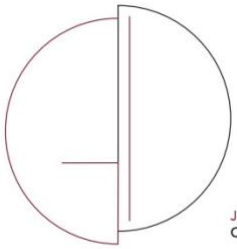

DIRITTO E NUOVE TECNOLOGIE*

Rubrica di aggiornamento dell'OGID.

Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Daniele Imbruglia nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulle Innovazioni Digitali, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (https://web.uniroma1.it/deap/ogid - jodi.deap@uniroma1.it).

SOMMARIO: ***1. La sentenza "Schrems II" del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo. – 2. Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore. – 3. CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo il provvedimento cautelare a favore di CasaPound. – 4. Pubblicate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell'Observatory on the Online Platform Economy. – 5. Lo studio del luglio 2020 su "Intelligenza Artificiale e responsabilità civile" commissionato dalla Commissione JURI del Parlamento europeo. – 6. Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR. – 7. La «Algorithm Charter » della Nuova Zelanda.***

* Contributo non sottoposto a referaggio ai sensi dell'art. 9, V co., del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 42 del 20.02.2019.

1. La sentenza "Schrems II" del 16 luglio 2020 della Corte di Giustizia UE sul Privacy Shield con gli USA e sulle clausole contrattuali tipo.

Il 16 luglio 2020 la Corte di Giustizia dell'Unione Europea ("**CGUE**") ha pronunciato la sentenza nel caso C-311/18 sul regime di trasferimento dei dati tra l'Unione Europea e gli Stati Uniti (c.d. "**Sentenza Schrems II**"). La Corte è intervenuta su due questioni: (i) la validità della decisione 2016/1250 della Commissione europea sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (c.d. *Privacy-Shield*) e (ii) la validità della decisione 2010/87 della Commissione europea sulle clausole contrattuali tipo ("**SCCs**").

La pronuncia segue la c.d. sentenza Schrems I del 2015 con cui, a seguito della denuncia del sig. Schrems in relazione al trasferimento dei suoi dati personali da Facebook Ireland a Facebook Inc., la CGUE aveva dichiarato invalida la decisione 2000/520 della Commissione europea che riteneva adeguato il livello di protezione garantito dal *Safe Harbour*. A seguito di tale sentenza, il sig. Schrems aveva formulato una nuova denuncia con cui chiedeva di vietare il trasferimento dei dati che Facebook Ireland continuava ad operare sulla base delle SCCs contenute nell'allegato della decisione 2010/87. Nel frattempo, la Commissione ha adottato la decisione 2016/1250 sull'adeguatezza del *Privacy-Shield*. La High Court irlandese ha quindi investito la CGUE della questione della validità di entrambe le decisioni.

Con riferimento alla decisione 2016/1250, la Corte ha evidenziato come questa riconosca il primato delle esigenze di sicurezza nazionale, interesse pubblico e rispetto della normativa statunitense. Pertanto, sulla base di tali esigenze, le autorità statunitensi sono legittimate ad accedere ai dati personali trasferiti da Paesi terzi. D'altra parte, non sono previsti limiti all'attuazione dei programmi di sorveglianza né garanzie per gli stranieri che ne siano oggetto, e non sono riconosciuti agli interessati diritti azionabili di fronte alle autorità statunitensi. Alla luce di ciò, la CGUE ha ritenuto che non sia garantito un livello di protezione equivalente a quello assicurato dal GDPR e, pertanto, ha dichiarato invalida la decisone 2016/1250.

Con riferimento alla decisione 2010/87, la Corte ha innanzitutto precisato che il livello di protezione delle SCCs deve essere valutato tenendo conto sia di quanto stabilito contrattualmente tra l'esportatore e il destinatario dei dati, sia delle garanzie previste dal sistema giuridico del Paese terzo con riferimento ad un eventuale accesso ai dati da parte delle autorità pubbliche. La Corte ha argomentato che non si possa ritenere invalida la decisione della Commissione sulla base del solo fatto che le SCCs, per la loro natura contrattuale, non vincolano le autorità di sicurezza del Paese terzo, ma è necessario stabilire se la decisione della Commissione preveda dei meccanismi che assicurino il livello di protezione richiesto e in particolare che assicurino che i trasferimenti di dati personali siano sospesi o vietati in caso di violazione delle clausole o dell'impossibilità di rispettarle. Al riguardo, la Corte ha osservato che la decisione 2010/87 ha riguardato SCCs che pongono in capo all'esportatore e al destinatario dei dati l'obbligo di verificare in via preliminare che il Paese terzo garantisca un livello di protezione adeguato, nonché l'obbligo, per il destinatario, di informare l'esportatore dell'eventuale impossibilità di rispettare le clausole con conseguente onere dell'esportatore di sospendere il trasferimento o di risolvere il contratto. Più in particolare, la Corte ha osservato che alla stregua delle SCCs formanti oggetto della decisione 2010/87 della Commissione, il titolare del trattamento stabilito nell'Unione, il destinatario del trasferimento di dati personali, nonché l'eventuale subincaricato di quest'ultimo, si impegnano reciprocamente a far sì che il trattamento di tali dati, compreso il loro trasferimento, sia effettuato e continuerà ad essere effettuato conformemente alla «normativa sulla protezione dei dati», ossia, secondo la definizione che compare all'articolo 3, lettera f), di tale decisione, «la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui è stabilito l'esportatore». E ha ulteriormente ritenuto che le disposizioni del GDPR, "lette alla luce" della Carta dei diritti fondamentali dell'Unione Europea, fanno parte di tale normativa. Alla luce di ciò, la Corte ha considerato valida la decisione in esame.

Il 17 luglio 2020 l'EDPB (*European Data Protection Board*) ha pubblicato una dichiarazione con la quale ha manifestato la sua approvazione della pronuncia della CGUE sottolineando al contempo la necessità di predisporre quanto prima nuovi strumenti e una nuova cornice per il trasferimento dei dati personali verso gli USA che sostituisca il *Privacy Shield* e garantisca il livello di protezione richiesto dal GDPR. Inoltre, il 24 luglio 2020 il medesimo *Board* ha pubblicato delle FAQ intese a fornire agli operatori i primi chiarimenti necessari per la prosecuzione del trasferimento di

dati verso gli USA alla luce della pronuncia della Corte.

CHIARA RAUCCIO

Sentenza CGUE
http://curia.europa.eu/juris/document/document.jsf;jsessionid=F88A37AF69B27E55D26CD174A97DF327?text=&docid=228677&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=15906436

EDPB *Statement*
https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_it

EDPB FAQ
https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en

2. Le conclusioni dell'Avvocato generale della Corte di Giustizia UE del 16 luglio 2020 sull'interpretazione delle direttive 2001/29/CE e 2000/31/CE sulla responsabilità dei gestori di piattaforme online con riferimento alle opere protette dal diritto d'autore.

Il 16 luglio 2020 l'Avvocato generale della Corte di Giustizia dell'Unione europea, Henrik Saugmandsgaard Øe, ha presentato le proprie conclusioni nell'àmbito delle cause riunite C-682/18 e C-683/18. Le osservazioni dell'Avvocato generale vertono sull'interpretazione dell'art. 3 della direttiva 2001/29, che riconosce agli autori di opere protette dal diritto di autore il diritto esclusivo di autorizzare o vietare qualsiasi "comunicazione al pubblico" delle medesime opere, e dell'art. 14 della direttiva 2000/31, che offre ai prestatori intermediari (cd. *hosting providers*) un esonero dalla responsabilità per le informazioni che essi memorizzano su richiesta degli utenti al ricorrere delle condizioni ivi previste. L'indagine non è stata invece estesa alla portata del nuovo art. 17 della direttiva 2019/790, entrata in vigore solo nel corso dei procedimenti principali interessati dal giudizio sottoposto alla Corte di Giustizia ("**CGUE**"), e dunque non applicabile alle relative controversie. Sul punto l'Avvocato generale, andando di contrario avviso rispetto alla tesi sostenuta dal Governo francese e da una delle persone fisiche in causa (il Sig. Frank Peterson), ha dichiarato che l'art. 17 della sopravvenuta direttiva 2019/790 (che dovrà essere attuata dagli Stati membri della UE entro il 7 giugno 2021 e che richiede ai gestori di piattaforme elettroniche di ottenere una autorizzazione dai titolari dei diritti, per esempio concludendo accordi di licenza) non è rilevante nemmeno dal punto di vista ermeneutico. In particolare, l'Avvocato generale ha affermato che con l'art. 17 di tale direttiva il Legislatore europeo non ha inteso fornire "un'interpretazione retroattiva dell'articolo 3, paragrafo 1, della direttiva 2001/29 e dell'articolo 14 della direttiva 2000/31", bensì ha "creato un nuovo regime di responsabilità per taluni intermediari online nel settore del diritto d'autore".
L'interpretazione delle citate disposizioni è stata sollecitata dalla Corte Federale di Giustizia tedesca (Bundesgerichtshof) nell'àmbito di due controversie, che possono così brevemente riassumersi:
i) nella prima (C-682/18) il Sig. Frank Peterson, produttore musicale, conveniva in giudizio la società YouTube LLC e la sua controllante Google LLC, lamentando la violazione del proprio diritto d'autore su diversi fonogrammi caricati sulla nota piattaforma YouTube da alcuni utenti senza la sua autorizzazione;
ii) nella seconda (C-683/18) la Società Elsevier Inc., gestrice dell'omonimo gruppo editoriale, conveniva in giudizio la società Cyando AG, dolendosi del caricamento sulla piattaforma di *hosting* e di condivisione di file Uploaded, gestita da Cyando, di diverse opere di cui la stessa Elsevier affermava di detenere i diritti esclusivi di sfruttamento. Anche in tale caso, le opere protette sono state messe in rete dagli utenti della piattaforma senza l'autorizzazione del titolare del diritto di privativa.
La Corte tedesca, sospendendo entrambi i giudizi, ha sottoposto alla CGUE, *inter alia*, le seguenti questioni:
1) se un gestore di una piattaforma di video su Internet come YouTube e un gestore di un servizio di condivisione di file come Uploaded, attraverso i quali gli utenti mettono a disposizione del pubblico video e file recanti contenuti protetti dal diritto d'autore senza il consenso degli aventi diritto, compiano un atto di "comunicazione" ai sensi dell'art. 3, paragrafo 1, della direttiva 2001/29;
2) in caso di risposta negativa alla prima questione, se i gestori di tali piattaforme possano beneficiare dell'esonero dalla responsabilità prevista dall'art. 14, paragrafo 1, della direttiva 2000/31;
3) se, a proposito delle informazioni che il prestatore memorizza su richiesta degli utenti del suo servizio, le condizioni alla cui ricorrenza è collegata la perdita del beneficio dell'esonero della responsabilità, consistenti, ai sensi dell'art. 14, paragrafo 1, lett. a), della direttiva 2000/31,

nell'essere il prestatore "effettivamente al corrente del fatto che l'attività o l'informazione [memorizzata] è illecita" e nell'essere "al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione [memorizzata]", debbano essere intese nel senso che tali condizioni debbono riferirsi a concrete informazioni illecite, cioè ad informazioni in particolare, o se, al contrario, sia sufficiente dimostrare che detto prestatore aveva una conoscenza o una consapevolezza generale e astratta del fatto che memorizza informazioni illecite e che i suoi servizi sono utilizzati per attività illecite;

4) se l'art. 8, paragrafo 3, della direttiva 2001/29 debba essere interpretato nel senso che la facoltà di chiedere un provvedimento inibitorio sia subordinata alla condizione di una cd. recidiva, ossia nel senso che l'inibitoria possa chiedersi solo se, a seguito della segnalazione di una violazione, essa non sia cessata o si sia verificata nuovamente.

In risposta al primo quesito, l'Avvocato generale chiarisce in primo luogo che quando un'opera protetta è condivisa in rete su di una piattaforma come YouTube, tale opera deve senz'altro considerarsi "messa a disposizione del pubblico" ai sensi dell'art. 3, paragrafo 1, della direttiva 2001/29: ogni internauta può liberamente accedervi, nel luogo e nel momento che egli preferisca. Sicché, se difetta la preventiva autorizzazione dell'autore dell'opera, la condivisione del contenuto integra una violazione del suo "diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico", previsto al citato art. 3.

Di tale violazione, però, a opinione dell'Avvocato generale, è "direttamente" responsabile solamente l'utente. Tanto perché è solamente l'utente a decidere se caricare un contenuto in rete, ovvero a decidere se trasmettere una determinata opera a un pubblico e avviare attivamente la "comunicazione"; per contro un tale ruolo – definito "imprescindibile" in richiamo alla giurisprudenza della Corte di Giustizia – non è mai ricoperto dai gestori della piattaforma online. Questi, invero, "non decidono, di propria iniziativa, di trasmettere opere a un pubblico", limitandosi a "segu[ire] le istruzioni impartite dagli utenti dei loro servizi": "Senza il loro [degli utenti, n.d.r.] intervento, i gestori delle stesse piattaforme non avrebbero nulla da trasmettere e il pubblico non potrebbe usufruire di dette opere". Essi sono cioè degli intermediari che, come previsto al considerando 27 della direttiva 2001/29, si limitano alla "mera fornitura di attrezzature fisiche" che consentono agli utenti delle loro piattaforme di realizzare la "comunicazione al pubblico" dell'opera.

Questa conclusione – precisa l'Avvocato generale – non esclude tuttavia che per i suddetti gestori di piattaforme online possa derivare una responsabilità definita "secondaria". Questione, questa, che deve essere esaminata alla luce delle norme in materia di responsabilità civile previste dagli Stati membri, nel rispetto dei limiti imposti dagli artt. 14 e 15 della direttiva 2000/31.

Quanto al secondo quesito, l'Avvocato generale suggerisce alla Corte di rispondere nel senso che il gestore di una piattaforma di condivisione di video, come YouTube, e il gestore di una piattaforma di hosting e di condivisione di file, come Uploaded, possono, in linea di principio, beneficiare dell'esonero previsto all'art. 14, paragrafo 1, della direttiva 2000/31 per qualsiasi responsabilità che possa derivare dai file che essi memorizzano su richiesta degli utenti delle loro piattaforme. A tale conclusione l'Avvocato generale giunge anzitutto constatando che, per entrambi i gestori delle piattaforme, risultano soddisfatte le due "condizioni cumulative" che circoscrivono l'àmbito di applicazione dell'art. 14: i) la prestazione di un "servizio della società dell'informazione" (art. 2, lett. a) della direttiva 2000/31); ii) tale servizio "consist[e] nella memorizzazione di informazioni fornite da un destinatario del servizio [...] a richiesta" di quest'ultimo. Peraltro, viene osservato che il servizio di memorizzazione, ai fini dell'applicazione dell'art. 14, non deve necessariamente essere "l'unico oggetto" o "l'oggetto principale" dell'attività dell'intermediario: come nel caso di Google – precisa l'Avvocato generale – il servizio di "memorizzazione di informazioni" può anche essere solo "uno dei numerosi aspetti della sua attività", fermo ovviamente restando che "l'esonero previsto in tale disposizione è, in ogni caso, limitato alla responsabilità che può derivare da tali informazioni e non si estende agli altri aspetti dell'attività del prestatore in questione".

L'Avvocato generale conclude per l'applicazione dell'art. 14 anche affermando che, nei casi oggetto di scrutinio, YouTube e Cyando non svolgono alcun ruolo cd. "attivo" che conferisca loro una conoscenza o un controllo delle informazioni memorizzate. L'Avvocato generale interpreta sul punto la nota giurisprudenza della Corte di Giustizia (v. Google France e L'Oréal/eBay) osservando che, per quelle pronunce, il "ruolo attivo" del gestore della piattaforma "si riferisce […] al contenuto stesso delle informazioni fornite dagli utenti": "Intendo la giurisprudenza della Corte nel senso che il prestatore svolge siffatto «ruolo attivo», tale da conferirgli «una conoscenza o un controllo» delle informazioni che memorizza su richiesta degli

utenti del suo servizio, qualora non si limiti a un trattamento di tali informazioni che sia neutro per quanto riguarda il loro contenuto, ma, per la natura della sua attività, acquisisca presumibilmente il controllo intellettuale di tale contenuto. Ciò si verifica se il prestatore seleziona le informazioni memorizzate, se esso è coinvolto attivamente nel loro contenuto in altro modo oppure se presenta tali informazioni agli occhi del pubblico in modo tale da farle apparire proprie. In tali ipotesi, il prestatore esce dal ruolo di intermediario delle informazioni fornite dagli utenti del suo servizio: esso se ne appropria". Nella specie – sempre secondo l'Avvocato generale – il ruolo "passivo" di YouTube non è escluso neppure dalla pacifica circostanza che tale piattaforma strutturi in modo particolare la presentazione dei video (inserendoli in una interfaccia di visualizzazione standard e indicizzandoli sotto varie rubriche) né dal fatto che venga fornita una funzione di ricerca e che venga effettuato un trattamento dei risultati di ricerca (anche fornendo una panoramica di "video raccomandati"). Viene osservato che controllare le condizioni di presentazione e visualizzazione dei risultati di ricerca non significa controllare "il contenuto delle informazioni ricercate".

In merito al terzo quesito, l'Avvocato generale suggerisce alla Corte di concludere dichiarando che l'art. 14, paragrafo 1, lett. a), della direttiva 2000/31 deve essere interpretato nel senso che le ipotesi ivi previste si riferiscono, in linea di principio, a informazioni illecite concrete. Pertanto, perché un prestatore possa perdere il beneficio dell'esonero di cui all'art. 14, non sarà sufficiente dimostrare che aveva una "conoscenza" o una "consapevolezza" generale e astratta del fatto che memorizza informazioni illecite e che i suoi servizi sono utilizzati per attività illecite. Tanto – secondo l'opinione dell'Avvocato generale – lo si deduce, oltre che dall'utilizzo nello stesso dettato dell'art. 14 di articoli determinativi ("l'attività o [...] l'informazione è illecita" e "l'illegalità dell'attività o dell'informazione"), anche dal contesto generale nel quale si inserisce la disposizione. Sul punto osserva l'Avvocato generale che il Legislatore europeo ha inteso stabilire un equilibrio tra i vari interessi in gioco, da un lato espressamente escludendo un generale obbligo del prestatore di sorvegliare le informazioni trasmesse o memorizzate e di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite (art. 15 della direttiva 2000/31); d'altro lato, non appena vengano effettivamente a conoscenza di un'informazione illecita, gravando i medesimi prestatori dell'obbligo di intervenire immediatamente per rimuovere tale informazione o per disabilitarne l'accesso, nel rispetto del principio della libertà di espressione e di procedure stabilite a tal fine a livello nazionale. In tale contesto l'art. 14, paragrafo 1, della direttiva 2000/31 "è quindi destinato a costituire una base per lo sviluppo, a livello degli Stati membri, di procedure cosiddette di «notifica e rimozione» (notice and take down) e le condizioni previste alle lettere a) e b) riflettono, pertanto, la logica di tali procedure: quando un'informazione illecita concreta è portata all'attenzione di un prestatore di servizi, questi deve eliminarla immediatamente".

Quanto all'interpretazione dell'art. 8, paragrafo 3, della direttiva 2001/29 – oggetto della quarta questione pregiudiziale – l'Avvocato generale suggerisce alla Corte di rispondere nel senso che tale articolo non richiede che si debba verificare una cd. "recidiva" per comportamento colpevole del prestatore al fine di richiedere l'intervento giudiziale.

Tanto perché, secondo l'Avvocato generale, le ingiunzioni contemplate da tale disposizione "non mirano (soltanto) a far cessare taluni comportamenti censurabili da parte loro [dei prestatori, n.d.r.]. Tale disposizione prende in considerazione anche intermediari «innocenti», nel senso che essi adempiono generalmente tutti gli obblighi loro imposti dalla legge. Essa consente ai titolari di diritti di pretendere dagli stessi un maggiore coinvolgimento nella lotta contro le violazioni del diritto d'autore commesse dagli utenti dei loro servizi, per il fatto che essi sono generalmente i più idonei a porre fine a tali violazioni. In quest'ottica, detta disposizione consente di imporre ai medesimi intermediari nuovi obblighi mediante ingiunzioni giudiziarie. Si tratta, in definitiva, di una forma di cooperazione forzata".

FRANCESCO BERNARDI

Conclusioni
http://curia.europa.eu/juris/celex.jsf?celex=62018CC0682&lang1=en&type=TXT&ancre=

Comunicato stampa
https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200096en.pdf

3. CasaPound vs. Facebook: il Tribunale di Roma conferma in sede di reclamo il provvedimento cautelare a favore di CasaPound.

Con ordinanza del 29 aprile 2020, avente per oggetto il reclamo ex art. 669 *terdecies* c.p.c.

avverso ordinanza resa dal Tribunale di Roma in data 11 dicembre 2019, il medesimo Tribunale, sez. XVII, ha confermato la pronuncia cautelare resa nella controversia tra CasaPound e Facebook iniziata il 9 settembre dello scorso anno, quando il noto social network procedeva alla disattivazione, senza preavviso, dell'account della Associazione di Promozione Sociale CasaPound Italia e, contestualmente, del profilo del suo dirigente nazionale ed amministratore della medesima pagina, adducendo, a motivo della disattivazione, la violazione delle condizioni d'uso, degli standard della community e, più in generale, della sua policy. In particolare, veniva richiamato «il divieto di presenza sulla piattaforma di "organizzazioni o individui che proclamano missioni violente o che sono coinvolti in azioni violente" e di diffondere messaggi di odio e discriminatori».

Ritenendo tale disattivazione illegittima, CasaPound e il suo dirigente nazionale agivano in giudizio contro Facebook, chiedendo, ex art. 700 c.p.c., un provvedimento cautelare d'urgenza per l'immediata riattivazione della pagina, indicando, relativamente al presupposto del *fumus boni iuris*, la violazione delle regole contrattuali da parte del social network e, con riferimento al *periculum in mora*, il grave pregiudizio sofferto sia in termini di danno all'immagine, determinato dalla chiusura della pagina del movimento ingiustamente accusato di diffondere odio, sia in quanto la disattivazione impediva l'esercizio di diritti fondamentali riconosciuti dalla Costituzione italiana.

Nel corso del procedimento cautelare – basato, come noto, su un giudizio sommario di cognizione e strumentale rispetto ad un successivo, ma solo eventuale, giudizio di merito – il Tribunale riteneva sussistenti entrambi i presupposti *supra* richiamati ed ordinava a Facebook Ireland Limited l'immediata riattivazione della pagina di CasaPound Italia e del profilo personale del suo amministratore. L'ordinanza muoveva dal rilievo «dell'importanza assunta da Facebook per chiunque intenda partecipare al dibattito politico e quindi per l'attuazione di principi cardine essenziali dell'ordinamento come quello del pluralismo dei partiti politici (art. 49 Cost.)». In ottemperanza a tale provvedimento, il 13.12.2019 Facebook riattivava le pagine de quibus.

Avverso codesta decisione, Facebook proponeva reclamo, respinto con l'ordinanza *de qua*, con cui il Collegio capitolino, dopo aver qualificato il rapporto tra Facebook e l'utente come un contratto atipico, nel quale il gestore fornisce gratuitamente un servizio e l'utente s'impegna a rispettare le condizioni del suo utilizzo, secondo il modello del contratto per adesione, predisposto per i clienti dalla parte fornitrice del servizio, statuiva, tra l'altro, che la disciplina del rapporto non può essere «rimessa senza limiti alla contrattazione fra le parti ed al rapporto di forza fra le stesse, né che l'esercizio dei poteri contrattuali sia insindacabile». Il ricorso al giudice per un bilanciamento degli interessi e per evitare gli abusi di diritto e di posizione della parte più "forte" sarebbe quindi necessitato, al fine di precludere «all'autonomia privata la limitazione a carico di uno dei contraenti dell'esercizio di diritti costituzionalmente garantiti», nel caso specifico la libertà di manifestazione del pensiero, protetta dall'art. 21 Cost., e la libertà di associazione, tutelata dall'art. 18 Cost.: «valori che nella gerarchia costituzionale si collocano sicuramente ad un livello superiore» rispetto alla libertà d'impresa (art. 41 Cost.) cui è riconducibile la posizione del gestore del servizio.

In conclusione, a parere dei giudici del riesame «non si ravvisano […] elementi che consentano di concludere che CasaPound sia un'associazione illecita secondo l'ordinamento generale», stante «l'impossibilità di riconoscere ad un soggetto privato, quale Facebook Ireland, sulla base di disposizioni negoziali e quindi in virtù della disparità di forza contrattuale, poteri sostanzialmente incidenti sulla libertà di manifestazione del pensiero e di associazione, tali da eccedere i limiti che lo stesso legislatore si è dato nella norma penale»; ma precisano che «la valutazione trova il suo limite nell'oggetto del presente giudizio, la verifica della compatibilità di CasaPound con la disciplina contrattuale riguardante le condizioni di utilizzo di Facebook alla stregua dei fatti e dei documenti allegati, non competendo a questo giudice la funzione di attribuire in via generale ad una associazione una "patente" di liceità, posto che condizione e limite dell'attività di qualsiasi associazione è il rispetto della legge, la cui verifica è rimessa al controllo giurisdizionale diffuso».

LUCIO CASALINI

https://www.corriere.it/cronache/20_maggio_29/casapound-contro-facebook-l-ordinanza-tribunale-roma-44eb8fae-a1ae-11ea-972c-41555f8ee621.shtml

4. Pubblicate il 10 luglio 2020 la relazione introduttiva e le prime tre bozze di relazione del gruppo di esperti dell'*Observatory on the Online Platform Economy*

Nel più ampio panorama della strategia volta a ridisegnare il futuro digitale dell'Unione Europea (v. la notizia n. 5 pubblicata su questa rubrica nel primo numero del 2020, e le notizie n. 1, 2, 3 e 4 pubblicate su questa rubrica nel secondo numero del 2020) la Commissione europea si è di recente fatta promotrice di una serie di iniziative che mirano allo studio e alla regolazione del settore della "*Online Platform Economy*". In particolare, l'esigenza di conoscere più a fondo questo fenomeno in rapidissimo sviluppo e di individuarne possibili criticità ha condotto alla costituzione di un "*Observatory for the Online Platform Economy*" [C(2018), 2393 final], composto da quindici esperti indipendenti di provenienza accademica. L'osservatorio ha una funzione prevalentemente consultiva nei confronti della Commissione in relazione ai trend principali del settore, con particolare attenzione all'emergere di condotte lesive da parte delle piattaforme nell'utilizzo degli algoritmi per i processi di *decision-making* e per il *ranking*, nell'accesso e nel trattamento di dati degli utenti e nelle relazioni *business-to-business*. Al gruppo di esperti è inoltre affidato il *follow-up* delle misure di regolazione già adottate dalla Commissione in questo settore [v., Regolamento (EU) 2019/1150 del Parlamento e del Consiglio Europeo del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, P2B (*Platform-to-Business*) - Regulation].

I lavori dell'osservatorio, iniziati il 26 aprile 2018, hanno portato il 10 luglio 2020 alla pubblicazione di una relazione introduttiva e delle prime tre bozze di *progress report*, corrispondenti ai primi tre dei cinque *workstreams* individuati dall'osservatorio: *(i)* l'individuazione di parametri economici per dimensionare correttamente il fenomeno delle piattaforme digitali, *(ii)* il problema del trattamento differenziato, *(iii)* l'accesso e l'utilizzo da parte delle piattaforme di dati. Ad essi si aggiungeranno poi *(iv)* gli *online advertising* e *(v)* l'analisi delle problematiche relative alle piattaforme con significativo potere di mercato. I *draft progress reports* nascono al fine di preparare il terreno di dibattito con i principali *stakeholders*, in vista della pubblicazione di un unico *report* finale entro l'ultimo trimestre del 2020 sulle potenzialità ed i rischi dell'economia delle piattaforme digitali.

La relazione introduttiva alle bozze di relazione, redatta dal Presidente del gruppo di esperti per l'osservatorio, Bruno Liebhaberg, muove anzitutto da una concettualizzazione lata di "*online platform economy*", inclusiva di ogni tipo di attività derivante da transazioni commerciali effettive o potenziali realizzate nel mercato interno ed agevolate, direttamente o indirettamente, dall'uso di piattaforme online, in particolare attraverso servizi di intermediazione online e motori di ricerca. I *players* di riferimento di questo mercato - principalmente *app stores*, *social media* e motori di ricerca - operano in qualità di intermediari fra due o più parti nello scambio di beni, servizi e informazioni. Gran parte del successo conseguito dalle piattaforme digitali si giustifica, dal lato consumatori, in virtù della facilitazione nell'accesso ai servizi e al sostanziale abbattimento dei costi del prodotto finali; dal lato professionisti, nell'incentivo loro garantito nel diversificare la propria offerta commerciale e nell'ampliarla sui mercati *cross-border*. Specialmente per le PMI, dunque, le piattaforme possono rappresentare un canale esclusivo di accesso al mercato a costi iniziali particolarmente contenuti.

Tuttavia, proprio con riferimento al legame che viene ad instaurarsi tra la piattaforma e i professionisti che decidono di avvalersene al fine di promuovere la propria offerta, il gruppo di esperti rivolge un primo monito alla Commissione. La prima relazione muove difatti dall'obiettivo di mettere in luce i parametri economici sulla cui base misurare l'effettivo volume dei *market-places* digitali, come mezzo per poter stabilire il grado di dipendenza del professionista alla piattaforma. In particolare, l'osservatorio individua per il settore in esame alcuni indici rivelatori di "*economic dependancy abuse*" da parte della piattaforma, fra i quali l'imposizione al professionista di costi particolarmente elevati per uniformarsi a certi standard tecnologici, l'alta percentuale delle commissioni percepite dalla piattaforma sull'importo complessivo del servizio erogato, nonché il rilievo che la piattaforma assume nell'attenzione del consumatore rispetto al soggetto che eroga il servizio o fornisce il bene. Alla luce di questo quadro, il report si conclude con alcune raccomandazioni rivolte alla Commissione di mappare questo fenomeno con più precisione, misurandolo non tanto in termini di valore aggiunto al prodotto interno lordo, quanto al volume degli scambi realizzati sulle piattaforme e al grado di dipendenza dei professionisti nell'utilizzo di questi strumenti per garantire l'erogazione dei propri servizi ai consumatori.

L'applicazione di termini iniqui nei rapporti P2B (*Platform-to-Business*) è inoltre all'origine, secondo l'osservatorio, di potenziali discriminazioni degli utenti sulle piattaforme e di trattamenti iniqui. Gran parte delle piattaforme esistenti sul mercato svolgono un ruolo "duale", tanto da porle in una posizione di naturale conflitto di interesse: da un lato, esse prestano un servizio neutrale di

intermediazione online e di motore di ricerca, dall'altro, offrono sul mercato propri prodotti, in competizione diretta con gli utenti business. Questa prassi è tuttavia ben nota alla Commissione europea che, chiamata a decidere su un caso di discriminazione del trattamento, ha condannato Google per aver applicato ai propri motori di ricerca criteri differenti e più favorevoli per l'indicizzazione dei propri servizi di "*shopping comparison*", rispetto ai criteri applicati ai servizi offerti da altri competitors [v. Case AT.39740 Google Search (Shopping), 27 June 2017, par. 699-700]. Il gruppo di esperti esprime inoltre preoccupazioni su talune pratiche invalse presso le piattaforme di maggiori dimensioni, volte alla realizzazione di strategie sistematiche a fini anticoncorrenziali, come l'acquisizione anticipata dei *newcomers* e il ricorrente mutamento di *policies* e condizioni negoziali. Tali condotte, oltre ad ingenerare confusione negli utenti dovuta alla mancanza di trasparenza dei servizi offerti, impongono alti costi di compliance in capo ai professionisti. Il report si conclude pertanto con l'interrogativo se le differenze che intercorrono fra i diritti municipali in ordine alla nozione di dipendenza economica non costituiscano un ostacolo alla uniforme applicazione del diritto europeo e possono dar così adito a discriminazioni nella tutela garantita a fronte di condotte abusive da parte delle piattaforme.

Il terzo ed ultimo monito rivolto da parte del gruppo di esperti riguarda l'accesso e l'utilizzo dei dati all'interno delle piattaforme digitali. I *data assets*, oltre a costituire la vera linfa vitale del funzionamento delle piattaforme, sono diventati una vera e propria moneta con la quale i consumatori pagano l'acquisto di numerosi servizi. Il *draft progress report* sui dati si concentra dunque sull'analisi e sulle diverse implicazioni del processo di acquisizione, di immagazzinamento e di utilizzo di dati da parte delle piattaforme, sul presupposto per cui gran parte degli utenti dispongono in modo particolarmente "incauto" dei dati che li riguardano, non conoscendone fino in fondo il valore effettivo. L'osservatorio muove dalle tradizionali ripartizioni dei *data assets*, per focalizzare l'attenzione su quelli di particolare rilievo per il settore della *platform economy*: informazioni che indentificano il professionista, gli effettivi ed i potenziali utenti (provenienza geografica, anagrafiche, etc.), informazioni sulle singole transazioni (prezzi, metodi di pagamento, comunicazioni interne) e sulle *performance* di ciascun professionista (volume di affari, traffico di utenti), attitudini del mercato e preferenze dei consumatori. Questi dati sono impiegati dalle piattaforme tanto in forma aggregata, quanto su base individuale. Se dal punto di vista economico è particolarmente ostico apprezzare il valore effettivo dei dati, in quanto il loro utilizzo è definibile "*non-rival*" – ossia, non preclude altri di servirsene allo stesso modo -, in ottica giuridica è nondimeno opportuno sviluppare una strategia diretta ad un'attenta *data governance*. L'osservatorio è dunque concorde nel proporre alla Commissione europea, in conclusione del proprio *report*, di evitare un approccio ai *data assets* sul modello "*one size fits all*", ma che tenga invece conto della eterogeneità dei dati di cui le piattaforme fanno uso e della varietà di scopi professionali per i quali si dispone degli stessi.

FEDERICO PISTELLI

Relazione introduttiva e tre bozze di relazioni
https://ec.europa.eu/digital-single-market/en/news/commission-expert-group-publishes-progress-reports-online-platform-economy
Observatory on Online Platform Economy
https://ec.europa.eu/digital-single-market/en/eu-observatory-online-platform-economy

5. Lo studio del luglio 2020 su "Intelligenza Artificiale e responsabilità civile" commissionato dalla Commissione JURI del Parlamento europeo.

Dopo il "Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))" del 27 aprile 2020 discusso durante la riunione della Commissione giuridica del Parlamento europeo (JURI) del 12 maggio 2020 (su cui v. la notizia n. 3 pubblicata su questa rubrica nel secondo numero del 2020), è stato pubblicato, con data luglio 2020, uno studio sullo stesso argomento commissionato dalla medesima Commissione JURI avente come titolo *Artificial Intelligence and Civil Liability*, il cui autore è Andrea Bertolini (lo "**Studio**").

Lo Studio affronta innanzitutto la questione della definizione di Intelligenza Artificiale (IA), soffermandosi sulla mancanza di una nozione generalmente condivisa e, dopo l'esame di qualche definizione "atecnica", tratta da dizionari e opere enciclopediche, presenta una tavola di comparazione, ordinata attraverso sette criteri, avente ad oggetto 14 definizioni "tecniche" di IA (ossia definizioni intese a formare la base per una regolamentazione), 11 delle quali rese da governi nazionali, una dall'OCSE, una dall'ISO e una dal

AI HLEG (il gruppo di esperti "di alto livello" sulla intelligenza artificiale, nominato dalla Commissione europea). Sulla base della predetta analisi, lo Studio suggerisce di rinunciare all'obiettivo di elaborare una definizione generale di IA, in linea con la tendenza registrata negli USA, e di proporsi piuttosto l'obiettivo di individuare modelli giuridici di responsabilità civile adeguati a specifiche applicazioni di IA. Viene sostenuto che le regole sulla responsabilità civile non possono essere unitarie, e che, in ragione delle differenze riscontrabili nelle varie applicazioni di IA, le regole sulla responsabilità debbano essere "*technology specific*" e, di conseguenza, differenziate.

Dopo aver argomentato a sostegno della tesi per cui le applicazioni basate sulla IA debbano considerarsi alla stregua di artefatti e quindi di prodotti (negando loro, di conseguenza, il riconoscimento di una soggettività o personalità giuridicamente rilevante), lo Studio ripercorre alcune questioni legate alle differenze di regime – a livello degli Stati membri della UE – tra i diversi modelli di responsabilità (contrattuale ed extracontrattuale), e si rivolge quindi alla direttiva sulla responsabilità da prodotti difettosi.

Ritiene che sia opportuno sollecitare una riforma della direttiva sulla responsabilità da prodotti difettosi che faciliti la posizione dell'utente vittima del danno, poiché l'opacità e la complessità di molte applicazioni basate sulla IA, rendono difficile, da un lato, l'individuazione del responsabile e la ripartizione della responsabilità tra più potenziali responsabili e, dall'altro, l'accertamento di un chiaro nesso di causalità tra una determinata condotta e il danno subìto dalla vittima, portando a scenari di «causalità alternativa».

Tuttavia, lo Studio evidenzia come anche una riforma della direttiva sulla responsabilità da prodotti difettosi rischia di non essere sufficiente per individuare, a livello europeo, una disciplina di responsabilità delle tecnologie IA perché, nonostante il suo àmbito applicativo sia teoricamente ampio, il costo e la complessità del contenzioso incentiva solo azioni di elevato valore, con il rischio di non tutelare adeguatamente gli utenti non professionisti che hanno subìto danni di modico valore dal malfunzionamento della tecnologia IA. Situazioni che sicuramente cresceranno di numero con l'aumento dell'automazione nella vita di relazione.

In ogni caso, si evidenzia che se, da un lato, una revisione della direttiva sulla responsabilità da prodotto difettoso sarebbe senz'altro auspicabile, dall'altro, l'impianto della medesima – definita "*technology neutral*" – non sembra poter consentire il conseguimento di una regolamentazione "*technology specific*", il cui pieno raggiungimento è, di converso, ritenuto necessario dallo Studio.

Dopo aver svolto tali considerazioni, il medesimo discute quale sia l'approccio europeo consigliabile per disciplinare i problemi di conflitto presentati dalle tecnologie di IA.

In primo luogo, esprime la convinzione che il quadro normativo debba essere affidato allo strumento dei regolamenti, piuttosto che a quello delle direttive, al fine di conseguire la massima armonizzazione possibile.

In secondo luogo, argomenta a favore della opzione di politica legislativa di dedicare regole *ad hoc* solo per quelle applicazioni che danno luogo a rilevanti preoccupazioni nella società civile. Sottolinea la necessità di promuovere l'uniformità di disciplina tra gli Stati membri, attraverso riforme in materia di responsabilità civile che siano adeguate a specifiche applicazioni di IA, confermando l'idea per la quale si ritiene inefficiente la creazione di una disciplina generale e astratta data la complessità dei fenomeni considerati.

Appare pertanto opportuno, secondo lo Studio, procedere verso normative *ad hoc* che disciplinino uniformemente la responsabilità civile relativa a specifiche tecnologie basate sulla IA.

Tuttavia, tenendo sempre in considerazione i princìpi di proporzionalità e sussidiarietà, lo stesso ritiene che solo quelle tecnologie che danno vita a rischi importanti e presentano preoccupazioni rilevanti per la società civile dovrebbero ricevere una disciplina specifica.

Quali tipi di applicazioni debbano essere regolamentati, e in quale ordine, è questione prioritaria da definire in base allo sviluppo tecnologico e alla diffusione sul mercato delle medesime applicazioni, bilanciando gli interessi e i benefici sociali legati a essa.

Lo Studio ricorda come negli anni recenti l'UE abbia adottato determinate regole sui droni e sulle piattaforme, e suggerisce che si debba continuare su questa strada monitorando più da vicino le nuove tecnologie emergenti, eventualmente attraverso un'agenzia dedicata o un gruppo di esperti, al fine di individuare quelle tecnologie che richiedono un pronto intervento. In ogni caso, raccomanda che gli interventi normativi siano specifici e ossequiosi dei princìpi di proporzionalità e sussidiarietà.

Su queste basi, propone che il principio informatore utile per l'individuazione dei soggetti responsabili debba consistere nel ritenere «strettamente» responsabile la parte che è maggiormente idonea a controllare e gestire il «rischio» legato alle tecnologie di IA, aggiungendo che tale principio debba essere applicato sulla base di «classi di

applicazioni» (c.d. metodo CbC: "*on a class-of-applications-by-class-of-applications basis*"), come definite dal c.d. approccio di gestione del rischio (c.d. RMA "*Risk-Management Approach*"), in linea con l'impostazione già adottata dalla direttiva sulla vendita e garanzia dei beni di consumo (direttiva 1999/44 CE).

Alla luce di quanto sostenuto, lo Studio esamina infine quattro campi di applicazione di tecnologie di IA: gli *industrial robot*, il *connected and automated driving*, le tecnologie diagnostiche dei *medical robot* e i droni.

A proposito di queste tecnologie, il medesimo trae alcune conclusioni per così dire comparative, osservando che mentre i robot industriali appaiono nel complesso regolamentati in modo adeguato – così che chi abbia subìto un danno ha un evidente e facile «punto di accesso» al contenzioso – per i veicoli connessi e a guida automatizzata sembra opportuno un intervento normativo a livello europeo per semplificare il complesso scenario che emerge dalla moltiplicazione dei soggetti potenzialmente responsabili e per evitare una frammentazione di discipline tra gli Stati membri. Raccomanda uno sforzo di armonizzazione per la regolamentazione dei droni, anche se reputa un intervento in questo settore meno urgente di quello nel campo dei veicoli a guida automatizzata. Segnala la necessità di dedicare un'attenta considerazione alle applicazioni di IA per la diagnosi in campo medico, osservando che se, da un lato, esse rappresentano una importante opportunità per migliorare l'assistenza medica, dall'altro lato l'attuale cornice regolamentare potrebbe penalizzare eccessivamente il personale sanitario. Infine, raccomanda di elaborare interventi normativi che abbiano lo scopo di proteggere i medici da eccessivi contenziosi e che introducano soluzioni alternative per risarcire le vittime, incluse forme di responsabilità di impresa.

ETTORE WILLIAM DI MAURO

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf

6. Il Consiglio di Stato francese conferma la sanzione di 50 milioni di Euro a Google per violazione del GDPR

Con sentenza del 19 giugno 2020, il Consiglio di Stato francese ha confermato la condanna al pagamento di 50 milioni di euro che la *Commission nationale de l'informatique et des libertés* (CNIL), ovvero l'autorità francese preposta alla tutela dei dati personali, aveva comminato alla società Google LLC con decisione del 21 gennaio 2019, per aver trattato i dati personali degli utenti in violazione delle disposizioni previste dal GDPR.

Il procedimento aveva avuto inizio su impulso delle denunce di due diverse associazioni di consumatori, *La Quadrature du Net* e *None of your business*, presentate a pochi giorni dall'entrata in vigore del GDPR.

Svolte le indagini del caso, l'Autority francese aveva giudicato la *privacy policy* del colosso americano non sufficientemente trasparente, poiché basata su un'informativa priva delle indicazioni necessarie alla formazione di un consenso degli utenti pieno e valido sul trattamento dei loro dati.

In particolare, è stato rilevato come durante la creazione di un account Google da un telefono con sistema operativo Android, le informazioni essenziali sulla finalità del trattamento, i periodi di conservazione dei dati e le categorie di informazioni utilizzate per la personalizzazione della pubblicità, non fossero sufficientemente chiare e accessibili, poiché distribuite e frammentate su diverse pagine da aprire e in più collegamenti su cui cliccare.

Le informazioni rese da Google, peraltro, risultavano insufficienti ed eccessivamente vaghe, tanto da non consentire all'utente una piena comprensione della portata del trattamento dei suoi dati, considerati la loro raccolta e il loro massiccio utilizzo da parte dei molti servizi offerti (Google Maps, You Tube, Gmail).

Ultima ma non meno importante criticità riscontrata dall'autorità garante francese è stata la mancanza del consenso validamente espresso dall'utente al trattamento dei suoi dati personali finalizzato alla personalizzazione della pubblicità.

L'accettazione delle condizioni prospettate nell'informativa resa, infatti, veniva rilasciata attraverso una casella pre-selezionata dal sistema, insieme all'accettazione dei termini e delle condizioni d'uso del servizio. Un consenso in blocco, dunque, in violazione del Considerando 32 del GDPR, che richiede un consenso prestato mediante un atto positivo inequivocabile (quindi non attraverso caselle di default già *flaggate*), idoneo a manifestare l'intenzione libera, specifica, univoca e informata dell'interessato di accettare il trattamento dei dati personali che lo riguardano.

Alla luce delle suddette considerazioni, il CNIL ha condannato la società americana al pagamento di una sanzione di 50 milioni di Euro.

Il ricorso presentato da Google dinanzi al Consiglio di Stato francese non ha avuto gli esiti sperati dal colosso di Mountain View. L'autorità giurisdizionale, infatti, ha confermato la decisione del CNIL, ritenendo la sanzione legittima e

proporzionata all'entità della violazione, dopo aver preliminarmente ritenuto sussistente la giurisdizione dell'autorità francese sulle operazioni di trattamento svolte dalla società tecnologica.
Nel ricorso, infatti, Google ha lamentato la carenza di giurisdizione del CNIL, asserendo che in ragione del fatto che la sua sede europea fosse localizzata in Irlanda, l'autorità competente dovesse essere quella irlandese.
Il Consiglio di Stato, tuttavia, ha ritenuto che quando l'autorità amministrativa francese ha avviato il procedimento, lo stabilimento irlandese non potesse qualificarsi quale stabilimento principale, in quanto esso non era coinvolto nelle operazioni di trattamento dei dati attuate nell'ambito del sistema operativo Android e dei servizi forniti da Google. Per questa ragione, i giudici francesi non hanno ritenuto applicabile il principio dello sportello unico (*one stop shop*), previsto dal GDPR, in base al quale i titolari dei trattamenti che operano in più Stati membri dell'Unione europea hanno come unico interlocutore l'autorità di controllo del paese dove hanno la sede principale.
Le decisioni delle autorità francesi hanno dato il via a un atteggiamento più rigoroso, che ha il merito di fornire un'effettiva tutela dei dati personali degli utenti digitali. Ai fini della corretta applicazione del GDPR, non potrà più ritenersi sufficiente un approccio meramente formalistico nell'elaborazione delle *privacy policy*.
Un passo importante lungo la strada - ancora tutta in salita - verso la piena consapevolezza (ancora apparentemente da acquisire) da parte dei cittadini su cosa si nasconde dietro l'utilizzo delle ormai sempre più svariate applicazioni, su quali dati vengono trattati, come, a quale fine, da chi e per quanto tempo, nonché su come questo possa incidere sui loro diritti fondamentali.
Deve anche tuttavia aggiungersi che la sanzione di 50 milioni di Euro comminata dal CNIL nel 2019 a Google risulta ad oggi un *unicum* non rilevandosi altre sanzioni precedenti e successive, minimamente comparabili nell'importo, irrogate da alcuna autorità europea per la protezione dei dati personali (compreso lo stesso CNIL), ciò che fa discutere circa l'effettivo *enforcement* delle disposizioni del GDPR in questo primo periodo di applicazione del regolamento.

SARA GARREFFA

https://www.cnil.fr/fr/le-conseil-detat-valide-la-sanction-prononcee-lencontre-de-la-societe-google-llc

7. La «*Algorithm Charter* » della Nuova Zelanda.

Il 28 luglio 2020, il governo neozelandese ha pubblicato la «*Algorithm Charter*» (la "**Carta**"), all'interno di un più ampio progetto inteso alla regolamentazione dei fenomeni connessi all'Intelligenza Artificiale. La Carta è definita come un «*evolving piece of work*», ed infatti è già stato pianificato un suo aggiornamento annuale al fine di adeguarne i contenuti alle novità legate al mondo digitale. Seppure la Carta è nata con l'obiettivo di definire standard regolatori per l'utilizzo degli algoritmi nel settore pubblico, essa presenta aspetti interessanti generalmente per ogni settore di impiego degli algoritmi.
La *ratio* di questo provvedimento risiede nella consapevolezza di un crescente ricorso a strumenti algoritmici nell'offerta dei servizi pubblici, unitamente ad una massiccia analisi e conservazione di dati, personali e non.
Come correttamente sottolineato nel documento, gli algoritmi possono generare soluzioni improprie sulla base di una loro non corretta programmazione od ampliare gli effetti negativi delle distorsioni valutative. Infatti, se da un lato, gli algoritmi offrono prospettive nuove e mezzi particolarmente incisivi nella modulazione dei modelli di business, dall'altra, essi possono essere portatori di rischi e preoccupazioni che vanno adeguatamente affrontati.
La Carta non fornisce una definizione univoca di algoritmo ma evidenzia l'eterogeneità dei significati che si possono attribuire a questo termine. Viene richiamato, inoltre, un precedente lavoro, il «*Government Use of Artificial Intelligence in New Zealand*», in cui si compie un più specifico approfondimento delle varie tipologie di algoritmi e di strumenti tecnologici e, in particolare, degli algoritmi predittivi.
La Carta si sofferma su due obiettivi principali: trasparenza (*trasparency)* e responsabilità (*accountability)* degli algoritmi. Garantire trasparenza e sicurezza nelle operazioni che utilizzano sistemi algoritmici rappresenta il principale obiettivo del documento. Si mette in risalto, infatti, che, mancando una uniformità nella gestione dei processi algoritmici, l'assenza di standard condivisi porta ad una frammentazione del quadro regolatorio e, di conseguenza, ad una rincorsa verso regole più blande.
Al momento della sottoscrizione della Carta, il governo neozelandese e le 21 autorità pubbliche aderenti hanno assunto l'impegno di rendere intellegibili le decisioni assunte dagli algoritmi, di verificare che l'analisi dei dati avvenga nel rispetto delle regole della privacy e della tutela dei diritti

fondamentali e di valorizzare l'intervento umano in simili processi automatizzati, conservando una particolare attenzione verso gli aspetti etici susseguenti. L'approccio, fortemente orientato ad attribuire centralità al ruolo dell'uomo, è, dunque, sintetizzato nei punti chiave della Carta: *Transparency*, *Partnership*, *People*, *Data*, *Privacy* – *Ethics* - *Human Rights* e, infine, *Human Oversight*.

In conclusione, il documento in esame ha il merito di proporre un accurato bilanciamento degli interessi coinvolti nella ricerca del delicato equilibrio tra innovazione ed esigenze di trasparenza, tra promozione del progresso tecnologico e necessità di preservare e tutelare i fondamentali diritti dell'uomo.

Ulteriore aspetto di rilevante interesse è il coinvolgimento diretto di vari operatori del settore pubblico. La presenza di questi ultimi garantisce, infatti, una più diffusa ed immediata applicazione dei nuovi standard delineati nella Carta.

Infine, è interessante notare che la prospettiva assunta all'interno del documento persegua il virtuoso obiettivo di adattare le regole ivi esplicitate alle mutevoli dinamiche del mercato digitale, distaccandosi volutamente da granitiche definizioni e accogliendo il principio di neutralità tecnologica.

ENZO MARIA INCUTTI

https://www.beehive.govt.nz/release/new-algorithm-charter-world-first