Relazione italiana del prof. avv. Alessandro Dario Cortesi – Saarbrücken – 5/10/2018

I.- La tutela della “privacy”
Il convegno di oggi ha per oggetto la “tutela dei dati personali”; tutela che ha ricevuto nuova attenzione ed impulso a seguito della pubblicazione del Regolamento UE 27 aprile 2016, n. 679.
Un aspetto merita di essere subito chiarito: la tutela dei dati personali è sovente associata a quella della privacy dell’individuo, ma si tratta di due aspetti che devono essere mantenuti distinti e separati.
Il concetto di “privacy”, che viene tradotto in italiano come “privatezza” o “riservatezza” (nella consapevolezza che si tratta di sostantivi che non riescono a rendere l’ampiezza di significato della parola inglese), è di origine anglosassone.
Si tratta di un istituto di fonte tipicamente dottrinale.
I trattati sul diritto alla privacy sono soliti richiamare il (davvero lungimirante) saggio di due giovani avvocati statunitensi, Samuel D. Warren e Louis D. Brandeis, pubblicato il 15 dicembre 1890 sull’Harward Law Review, intitolato appunto “The right to Privacy” , ma si trattò, è ovvio, solo di uno spunto preliminare.
Assai più significativi per il riconoscimento di tale diritto furono gli interventi, di oltre mezzo secolo successivi:
• di William Faulkner, in un’opera intitolata “Privacy” , apparsa negli USA nel 1955, in cui premio Nobel per la letteratura si scagliava con massima veemenza contro il tritacarne mediatico (all’epoca alla spasmodica ricerca dei dettagli della sua vita amorosa);
• e soprattutto di William L. Prosser, in un’opera anch’essa intitolata “Privacy”, apparsa nell’agosto del 1960 sulla California Law Review.
In un curioso rimpallo fra la East Coast e la West Coast degli Stati Uniti, infatti, l’idea iniziale, espressa dai giovani avvocati di Boston, che teorizzavano il “right to be let alone” (ovvero il diritto ad essere lasciati soli per godere della propria intimità, nella determinazione delle proprie scelte di vita, nell’espressione della propria sensibilità, del proprio credo, nella custodia dei propri pensieri ed emozioni), veniva ripresa settanta anni dopo da Prosser, preclaro preside dell’University of California – School of Law di Berkeley, autore di fondamentali monografie sui torts, che così tipizzava le sue possibili violazioni:
a) penetrare in uno spazio chiuso riservato;
b) rivelare in pubblico i fatti privati;
c) mettere qualcuno in cattiva luce;
d) appropriarsi a fini commerciali del nome o dell’immagine di un privato, senza che questi abbia prestato il consenso.
È evidente, quindi, che il diritto alla privacy, nato come baluardo dell’individuo (tutela di livello costituzionale) contro illegittime intromissioni del potere pubblico, si stesse trasformando, nell’interpretazione della dottrina più autorevole, in uno strumento di difesa anche da ingerenze dei privati.

Si trova conferma di tale lettura nella Dichiarazione universale dei diritti dell'uomo, adottata dall'Assemblea Generale delle Nazioni Unite il 10 dicembre 1948, che stabilisce all'art. 12 che "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie [da chiunque perpetrate, quindi – N.d.A.] nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".
Le costituzioni degli Stati europei furono molto più restie nel recepimento delle dottrine anglosassoni, così come le relative giurisprudenze. Soprattutto in Italia, il desiderio di superare le prassi censorie del famigerato Ministero della Cultura Popolare di epoca fascista impedì di riconoscere, expressis verbis, il diritto alla privacy.
La Carta Costituzionale italiana, pubblicata in Gazzetta Ufficiale 27 dicembre 1947, n. 298, sancisce solennemente l'inviolabilità della libertà personale (art. 13), l'inviolabilità del domicilio (art. 14) e di ogni forma di comunicazione (art. 15), la libera manifestazione del pensiero (art. 21), disposizioni che limitano l'intervento pubblico ad ipotesi eccezionali, stabilite dalla legge.
Non viene però esplicitato un diritto del cittadino alla riservatezza e, quanto alla stampa, all'art. 21, secondo comma Cost., si precisa viceversa che essa "non può essere soggetta ad autorizzazioni o censura" .
Una prima esplicitazione del diritto alla riservatezza è rinvenibile, invece, nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950 e ratificata in Italia con legge 4 agosto 1955, n. 848.
La Convenzione prevede, infatti, all'art. 8 "Diritto al rispetto della vita privata e familiare" che "1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui".
Come si vede, però, ancora a quell'epoca l'attenzione dei giuristi si appuntava principalmente sul diritto alla riservatezza. In Italia, ancora negli anni Cinquanta, la riflessione dottrinale si concentrava sulla tutela delle vittime dell'esposizione mediatica: si avanzavano critiche sull'ingerenza dei media nei casi nostrani Caruso, Petacci, Soraya.
Sono solo le Costituzioni più "giovani" che hanno introdotto delle disposizioni specifiche in materia di privacy.
Si ricordano:
• la Constituição da República Portuguesa del 2 aprile 1976 (cfr. art. 35, più volte novellato);
• la Constitución española del 27 dicembre 1978 (cfr. art. 18, comma 4);
• la Costituzione olandese del 17 febbraio 1983 (cfr. art. 10);
• le Costituzioni dei Länder tedeschi;
• le Costituzioni di molti paesi dell'Europa dell'Est;
• la Costituzione greca (cfr. art. 9A nella sua revisione del 2001).

* * * *

II.- L'emersione nelle Carte dei diritti dell'uomo della distinta tutela dei "dati personali"

Se si procede con un secondo balzo storico, e ci si proietta negli anni Novanta, si registra l'emersione di un secondo approccio, al cui sviluppo le istanze europee hanno contribuito in misura rilevante. Secondo tale visione non vi può essere concreta tutela della vita privata, se non si tutelano anche i dati personali.

Se si esamina ad esempio la Carta dei diritti fondamentali dell'Unione Europea, che in Italia è nota come Carta di Nizza (essendo stata ivi solennemente proclamata il 7 dicembre 2000), si nota che essa non dedica più un solo articolo alla questione, bensì due: il settimo e l'ottavo.

Per inciso, come tutti loro ricorderanno, detta Carta è stata sottoscritta (in versione adattata) a Strasburgo il 12 dicembre 2007 e, ai sensi dell'art. 6 del trattato di Lisbona, ha acquisito il medesimo valore giuridico dei trattati.

Ebbene l'art. 7 della Carta, rubricato "Rispetto della vita privata e familiare" precisa che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni", il che riflette l'approccio anglosassone originario.

Ma il successivo art. 8, rubricato "Rispetto dei dati di carattere personale" specifica invece che "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o un altro fondamento legittimo previsto per legge. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano e di ottenere la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

* * * *

III.- La centralità dei dati nell'era dell'accesso. I c.d. big data.

Non vi è bisogno di spendere troppe parole per illustrare la pervasività della rivoluzione tecnologica che segna in profondità la società in cui viviamo. Praticamente ogni aspetto della nostra vita è toccato dall'informatica. In altre parole, utilizzando un acronimo invalso nella prassi, tutto è ITC, information and communication technology, tecnologia dell'informazione e della comunicazione.

Non si tratta della prima rivoluzione dell'informazione. Gutenberg intorno al 1439 inventò la stampa (risale al 1455 la pubblicazione della Bibbia, primo libro di una certa rilevanza stampato con caratteri mobili a Magonza). Secondo alcuni storici, nei cinquant'anni compresi tra il 1453 ed il 1503, furono stampati circa 8 milioni di libri, più di quelli che avevano prodotto tutti gli emanuensi d'Europa dalla fondazione di Costantinopoli, ovvero 1200 anni prima.

Oggi vengono processati ogni giorno zettabyte di dati (1 ZB= 1021 byte): basti pensare alle fotografie scattate, alle e-mail scambiate, ai post pubblicati sui social network, ma anche ai dati raccolti dai satelliti, alla criptovaluta trasferita ed alle relative trascrizioni su blockchain.

Oggi come allora l'incremento esponenziale della mole di dati trattati e della velocità con cui si producono è cagionata da innovazioni tecnologiche. Non

una soltanto, per la precisione: lo sviluppo di elaboratori elettronici sempre più performanti, la precipitazione del costo delle memorie di massa e dei sensori, il collegamento dei computer in rete (ed in primis internet), la telefonia cellulare (gli smartphone), la compressione dei dati, la globalizzazione, sono tutti fattori concorrenti.
Ma decisivi appaiono la digitalizzazione (digitization), ovvero la conversione di un'informazione in formato digitale, e la c.d. datizzazione (datafication), ovvero la trasformazione in dati pienamente manipolabili.
Per comprendere la differenza fra questi due concetti vi propongo l'esempio dei documenti di testo.
L'acquisizione in formato immagine di una pagina di un libro (scansione/scannerizzazione) ha come risultato un file che riproduce il testo. Quel file può essere copiato, spedito, manipolato (nel senso che l'immagine può essere ridotta, ampliata, tagliata ecc.). Il risultato della scansione non è ancora però un file di testo, compiutamente modificabile dall'utente. Chi usufruisce del file non può copiarne dei brani ed incollarli in un altro documento; non può cancellare delle parole e sostituirle con altre o aggiungere delle righe.
Per ottenere questo risultato non basta uno scanner. È necessario utilizzare un programma di riconoscimento ottico dei caratteri, ovvero un software in grado di riconoscere i segni grafici ed interpretarli quali lettere dell'alfabeto (cd. software OCR – Optical Character Recognition).
Il procedimento da ultimo descritto attua la datizzazione.
Con queste tecniche tutto viene trasformato in dati: intere biblioteche, interi cataloghi musicali, collezioni di fotografie e di audiovisivi. Come anticipava il noto sociologo Jeremy Rifkin, questo consente di passare dall'"era della proprietà", all'"era dell'accesso" e dà l'abbrivio all'economia della condivisione (sharing economy).
È facile preconizzare che su questa strada che non si registreranno marce indietro.
Si diffonderanno sempre più i c.d. wearable devices (ovvero gli elaboratori indossabili), come i vari orologi e attrezzature fitness, che monitorano in tempo reale lo stato di salute dell'individuo. Ogni cosa sarà dotata di sensori e collegata alla rete (c.d. internet of things). Sono già in commercio elettrodomestici che implementano la c.d. domotica. Alcuni giorni fa ho visto in un negozio persino uno spazzolino da denti che si collega alla rete.
Appositi visori (come i Google Glass) permetteranno di sperimentare la c.d. realtà aumentata, ovvero di ottenere in tempo reale una serie di approfondimenti in relazione a quanto stiamo vedendo (ma nel contempo accenderanno miliardi di telecamere in grado di registrare ogni nostro movimento).
Si diffonderanno i visori di realtà virtuale che ci consentiranno di lavorare, relazionarci con gli altri distanti anche migliaia di chilometri, frequentare lezioni, fare la spesa, assistere a funzioni religiose e magari assistere ai convegni della nostra associazione, rimanendo nella nostra abitazione e condividendo immaginifici spazi in grado di appagare al meglio i nostri sensi.
E poi si svilupperanno i veicoli a guida autonoma, i robot umanoidi e così via.

Tutti queste attrezzature potranno funzionare solo processando enormi moli di dati e contribuiranno a crearne altrettante.
Ma se questi aspetti, seppur futuristici, sono intuiti dalla collettività, altri lo sono assai meno.
L'uomo è abituato da sempre ad assumere delle decisioni fondate su di una serie di informazioni limitata. Il pensiero umano razionale prende le mosse dall'osservazione di determinati fenomeni, formula congetture, estrapola dalla variegata realtà dei dati che ritiene rilevanti, eventualmente analizza delle statistiche (possibilmente rappresentative dell'universo) ed infine verifica se le ipotesi iniziali trovino o meno conferma. Laddove le ipotesi iniziali vengano smentite dalla sperimentazione, si cerca di affinarle, in un ciclo continuo che tende a scoprire una nuova legge naturale (sempre ammesso che la natura segua delle leggi e non sia dominata dal caos).
I big data consentono agli elaboratori di procedere diversamente, di assumere delle decisioni processando praticamente tutti i dati, qualsivoglia variabile, nessuna esclusa. Questo modo di procedere già oggi rende più efficiente il medico diagnostico di IBM rispetto ad un dottore in carne ed ossa; già oggi rende alcuni sistemi esperti, utilizzati dagli studi legali, più efficienti di una schiera dei più preparati legali.
Gli elaboratori sono in grado di individuare delle corrispondenze fra fenomeni che l'uomo non aveva finora mai colto (e che solo la capacità di calcolo delle macchine può disvelare). Si sono così evidenziate delle relazioni fra alcuni sintomi e determinate malattie, o fra la somministrazione di determinate molecole e degli esiti medici positivi: corrispondenze (schemi ripetitivi, in inglese pattern) che raggiungono elevatissimi gradi di probabilità (quasi certezze), ma di cui tuttora si ignora completamente la ratio. In altre parole con queste tecniche siamo in grado di curare malattie, senza sapere come sia possibile.
Passando ad argomenti più vicini ai nostri domini di esperienza, anche a Milano si sono messi alla prova degli algoritmi di c.d. polizia predittiva (ad opera della società Keycrime) in grado, una volta processati moltissimi dati relativi ai reati ed ai soggetti che li hanno commessi (11.000 variabili per ogni reato), di prevedere quando e dove si verificheranno nuovi crimini e quindi di sventarli. L'impiego di tali algoritmi ha consentito di abbattere significativamente il numero delle rapine: le forze dell'ordine si fanno trovare puntuali all'appuntamento con il rapinatore, come se avessero ricevuto una soffiata.
E ancora non è tutto. L'intelligenza artificiale, come sappiamo, rappresenta il tentativo di emulare il cervello umano. La nuova frontiera è quella del c.d. machine learning, ovvero del software che autoapprende (id est che si riprogramma in piena autonomia).
Esiste il concreto rischio che determinate funzioni, anche decisive per la sopravvivenza dell'uomo (si pensi alla gestione del triage nel pronto soccorso), vengano demandate a computer, che dimostrano di ottenere risultati di massima efficienza, in ragione di algoritmi che si aggiornano in tempo reale con una velocità tale che non è fisicamente consentito ad un programmatore umano comprenderne il funzionamento. Presto si porrà quindi questo dilemma:

sarà meglio affidarci alle macchine, perché anche se non ne comprendiamo fino in fondo le ragioni, ottengono risultati irraggiungibili dalla mente umana, o mantenere la nostra autonomia?
Preferireste essere giudicati da un giudice in carne ed ossa, nella consapevolezza che la sua umanità porta con sé la possibilità che commetta errori, o dalla fredda lucidità ed imparzialità di un giudice computer (secondo esperienze che vengono già condotte ad es. in Cina)?
* * * *
IV.- Le direttive sulla tutela dei dati personali ed il Regolamento europeo.
Dal momento che la circolazione dei dati, a tacer d'altro, è alla base del commercio elettronico, le istituzioni europee si sono rapidamente rese conto della necessità di armonizzare le nascenti discipline nazionali e ciò innanzitutto per creare un maturo mercato unico europeo .
Non possiamo per ragioni di tempo esaminare nel dettaglio le numerose disposizioni che sono state emanate per perseguire tale scopo.
Fra le principali citiamo:
• la direttiva 1995/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (attuata in Italia con legge 31 dicembre 1996 n. 675) e
• la direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (recepita in Italia con Decreto delegato legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali).
A distanza di oltre 20 anni dalla precedente fonte europea in argomento, le istituzioni europee hanno operato una scelta diversa: in luogo di un'ulteriore direttiva, si è scelto di emanare il Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (d'ora in poi GDPR).
Il fatto stesso che si sia scelto di riformare la materia attraverso un regolamento (fonte che, a differenza della direttiva, non necessita della mediazione dei singoli Stati, ma si impone direttamente nei loro ordinamenti), prova che la desiderata uniformazione non si sia compiutamente raggiunta, il che è del resto ammesso nel considerando 9 dello stesso GDPR.
Il Regolamento avrà maggiori possibilità di successo? Nutro alcuni dubbi a proposito.
A tacer d'altro l'inasprimento delle sanzioni (che ai sensi degli artt. 83 e 84 dovranno essere effettive, proporzionate e dissuasive), la previsione della figura del Responsabile della protezione dei dati (artt. 37 e ss.), l'esplicitazione dei principi di responsabilizzazione (accountability: considerando 57 e art. 5 c. 2), di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25) hanno ridestato l'interesse delle imprese, sensibilizzate al riconoscimento di questi diritti anche se il trattamento è effettuato al di fuori dell'Europa (nei limiti indicati dall'art. 3).
Questi principi innovativi faciliteranno la circolazione dei dati in ambito sovranazionale, ma è lecito dubitare che si raggiungerà, anche tramite il Regolamento, il traguardo di una disciplina davvero uniforme e ciò nonostante

il ruolo sempre più forte che sono chiamate a svolgere:
• le Autorità garanti nazionali;
• il Gruppo di lavoro ex articolo 29 (della direttiva 95/46/CE), ora ridenominato European Data Protection Board (in italiano Comitato europeo per la protezione dei dati);
• il Garante Europeo della protezione dei dati.
e nonostante l'attività degli Organismi di certificazione di cui all'art. 43 del GDPR e la redazione dei codici di condotta di cui all'art. 40 GDPR.
Ostacola il raggiungimento di questi obiettivi il dato letterale del GDPR, che risulta assai farraginoso, ripetitivo e talvolta oscuro (problema a cui si aggiunge la complessa traduzione in lingua italiana di alcuni sintagmi che complica l'attività dell'interprete).
Ma soprattutto la consapevolezza che il diritto alla tutela dei dati personali non può essere riconosciuto quale diritto assoluto.
Anche se è accordata all'individuo la facoltà di decidere se e in che misura rendere disponibili informazioni sul proprio conto ed il potere di controllarne la successiva circolazione, la Corte di giustizia in una serie di pronunce (cfr. ad es. sentenza 9 novembre 2010 in cause riunite C-92/09 e C-93/09, Volker und Markus Schecke e Eifert e sentenza 5 maggio 2011, C-543/09) ha chiarito che tale diritto non si può tradurre in una sorta di signoria sui dati personali a sé riferiti, così da orientarne arbitrariamente o capricciosamente la circolazione.
Assai chiaro in questo senso è il considerando 4 del GDPR laddove specifica che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità".
Anche il Regolamento, quindi, riconosce l'esistenza di interessi pubblici confliggenti (cfr. ad es. considerando 16 e 19) e la necessità di operare un bilanciamento, entro degli spazi in cui si concretizzano le scelte politiche nazionali (cfr. art. 2, comma 2 GDPR).
Questa la ragione per cui permangono nel testo del Regolamento frequenti rinvii al diritto degli Stati membri (si vedano, e senza pretese di esaustività, i considerando 8, 10, 19, 121, 129, 142, 146, 152, 153, 154, 155, 163 e gli artt. 6, 8, 9, 14, 15, 28, 29, 32, 36, 37, 38, 39, 40, 42, 43, 49, 53, 54, 62, 80, 85) e si aprono quindi ampi spazi per il permanere di discipline nazionali difformi.
* * * *
V.- L'attuazione in Italia del GDPR
L'attuazione del GDPR in Italia è stata (ed è) tortuosa.
Nonostante il Regolamento europeo offrisse un biennio di tempo per armonizzare le discipline interne, il Governo italiano ha ottenuto una delega in questo senso dal Parlamento solo 6 mesi prima, con legge 25 ottobre 2017 n.163 (legge di delegazione europea 2016-2017, cfr. art. 13).
Il 14 dicembre 2017 la collega dell'Università di Bologna, prof.ssa Giusella Finocchiaro, è stata chiamata dal Ministero della Giustizia a presiedere un Gruppo di lavoro per l'esercizio della delega. In conclusione dei propri lavori, condotti in tempi assai rapidi, il Gruppo di lavoro ha predisposto un articolato interessante. In una logica di accesa semplificazione delle fonti il Gruppo

suggeriva, fra l'altro, la completa abrogazione del Codice in materia di protezione dei dati personali.
Personalmente ho appoggiato tale soluzione, ma ho sostenuto, come in verità la maggior parte degli interpreti, che a legge immutata essa fosse di dubbia costituzionalità per eccesso di delega.
Forse anche per questa ragione, l'Esecutivo non ha accolto la proposta del Gruppo di lavoro e la delega, che aveva naturale scadenza il 21 maggio 2018 (pochi giorni prima rispetto al fatidico 25 maggio 2018, termine di piena applicazione del GDPR), non è stata esercitata nei termini (con conseguenze assai problematiche in particolare in relazione alle sanzioni, comprese quelle penali).
Tuttavia l'art. 13 comma 3, prevedeva che il Governo esercitasse la delega secondo le procedure previste dall'art. 32 della legge 24 dicembre 2012, n. 234. Questa norma, a sua volta, specifica che quando gli schemi dei decreti delegati vengano inviati alle Commissioni parlamentari per il previsto parere quando manchino meno di 30 giorni alla scadenza della delega, come è accaduto nel caso di specie, tale scadenza risulti automaticamente prorogata per la durata di tre mesi (quindi fino al 21 agosto 2018).
Questa interpretazione ha consentito al Governo di esercitare la delega in tempi più recenti ed emanare il decreto delegato legislativo 10 agosto 2018, n. 101 (la cui pubblicazione tutti noi cultori della materia abbiamo atteso con ansia questa estate).
La pubblicazione del decreto è avvenuta solo nella Gazzetta Ufficiale 4 settembre 2018, n. 205. Il codice in materia di protezione dei dati personali D. lgs. 196/2003 cit. non solo non è stato abrogato ma è stato radicalmente novellato. Le nuove disposizioni sono entrate in vigore, a seguito della vacatio legis, solo pochi giorni fa e precisamente il 19 settembre 2018.
* * * *
VI.- Il ruolo dell'amministrazione
Non vi è dubbio che le pubbliche amministrazioni detengano sterminate moli di dati. Basti pensare ai censimenti dell'istituto nazionale di statistica, all'anagrafe della popolazione, alle liste elettorali, ai dati catastali, al pubblico registro automobilistico, alle dichiarazioni dei redditi, alle cartelle mediche.
Atteso che le pubbliche amministrazioni conservano i dati personali solo in quanto indispensabili per l'esercizio delle funzioni amministrative, si tratta di trattamenti legittimati a prescindere dal consenso dell'interessato e ciò in forza dell'art. 6, comma 1 GDPR, lettere c) (obbligo legale del titolare del trattamento), d) (salvaguardia di interessi vitali) e soprattutto e) (esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).
La superfluità del consenso semplifica le cose, ma le pubbliche amministrazioni devono comunque individuare un ufficio che si occupi dell'adeguamento al GDPR (in primis che si occupi della tenuta del registro dei trattamenti, art. 30 GDPR e dell'aggiornamento delle informative, artt. 13 e 14 GDPR), il che costituisce un processo continuo. Esse devono nominare un Responsabile della protezione dei dati personali (art. 37 GDPR), figura peraltro con caratteristiche assolutamente peculiari, che viene tipicamente nominata a seguito di procedura ad evidenza pubblica (integrando un appalto di servizi).

E soprattutto devono implementare adeguate misure di sicurezza per fronteggiare aggressioni di qualsiasi genere, non solo quelle di hackers e cyberterroristi, ma anche quelle, spesso assai trascurate, che utilizzano tecniche di c.d. ingegneria sociale (social engineering).
Se Facebook, che investe milioni di dollari in sicurezza – notizia di qualche giorno fa –, ha registrato negli ultimi giorni la violazione dei dati personali di 90 milioni di account (fra cui quello del vostro relatore di oggi), possiamo immaginare che difese implementino i nostri comuni più piccoli. Non si tratta di rischi solo teorici: alcune anagrafi sono state colpite ad es. dai c.d. cryptoransomware, software che criptano tutti i dati e chiedono un "riscatto" in bitcoin…
Vi sono poi interi settori di trattamento che sono regolati da disposizioni specifiche (cfr. Capo IX GDPR). Si pensi, ex plurimis, ai dati personali in ambito penale (disciplinati dal D. lgs. 18 maggio 2018, n. 51), ai dati in ambito sanitario, ai dati trattati ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o ai fini statistici (cfr. art. 89 GDPR).
Le maggiori criticità che le amministrazioni devono affrontare sono rappresentate tuttavia, secondo la mia esperienza, dalle intersezioni fra la disciplina della tutela dei dati personali e le disposizioni in tema di:
1) accesso alla documentazione amministrativa (su cui v. prossimo paragrafo);
2) trasparenza (disciplinata in Italia dal Decreto legislativo 14 marzo 2013, n. 33 di Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni);
3) dematerializzazione della documentazione amministrativa (disciplinata in particolare dal Decreto legislativo, 7 marzo 2005, n. 82, c.d. Codice dell'Amministrazione Digitale).
Dal punto di vista organizzativo, l'art. 17, comma 1 del Codice dell'Amministrazione Digitale prevede la nomina del Responsabile della transizione digitale dell'amministrazione. Detto soggetto dovrà ovviamente confrontarsi con i responsabili sopra citati e con altre funzioni apicali indicate nello stesso Codice (cfr. art. 44 comma 1-ter CAD).
Anche se l'art. 20, comma 3 del GDPR esclude il diritto alla portabilità dei dati necessari per l'esecuzione di un compito di interesse pubblico, il Codice dell'amministrazione digitale, all'art. 50, continua a richiedere che i dati siano "formati, raccolti, conservati, resi disponibili ed accessibili" secondo modalità che consentano l'utilizzo da parte delle altre pubbliche amministrazioni e dei privati. E non potrebbe essere altrimenti: la partecipazione al procedimento amministrativo informatico (art. 4 CAD), la partecipazione democratica elettronica (art. 9 CAD), non sarebbero altrimenti predicabili.
Si comprende così la ragione per cui l'art. 68 CAD richieda, per la scelta del software da parte delle pubbliche amministrazioni, di valutare comparativamente le varie soluzioni disponibili, considerando anche l'utilizzo del free software (di formati non proprietari).
Si applica, invece, anche alle pubbliche amministrazioni l'art. 22 GDPR che dispone che "L'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la

profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Il comma 3 prescrive "il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".
Si tratta a mio avviso di una delle disposizioni più significative del Regolamento Europeo, che rappresenta una difesa nei confronti di quelle che sono state qualificate ad es. da Cathy O'Neil, in una recente opera , come "armi di distruzione matematica" (si pensi all'esempio del triage ospedaliero di cui sopra), ma, per le amministrazioni che hanno in corso processi di digitalizzazione ed efficientamento delle proprie funzioni, può segnare un rilevante ostacolo.
* * * *
VII.- La tutela giurisdizionale
Volgendo lo sguardo alla tutela giurisdizionale, la scelta del legislatore italiano è stata tradizionalmente quella di attribuire le controversie relative alla protezione dei dati personali al Giudice ordinario.
È prevista, invero, anche una forma di tutela amministrativa ai sensi degli artt. 140-bis e ss. del Codice per la tutela dei dati personali: si può presentare reclamo all'Autorità Garante, che decide entro nove mesi. Ma avverso la decisione del Garante è comunque ammesso ricorso giurisdizionale (cfr. art. 143, u.c. Codice).
L'art. 10 del D. lgs. 1° settembre 2011 n. 150, nel testo che è stato vigente dal 6 ottobre 2011 al 18 settembre 2018, prevedeva la competenza del tribunale del luogo ove avesse residenza il titolare del trattamento dei dati. A seguito della novella del 2018, risulta competente in alternativa il Tribunale del luogo di residenza dell'interessato (scelta più razionale, che avvicina queste controversie a quelle che concernono la tutela dei consumatori).
Il rito da seguirsi è quello semplificato del lavoro, ma la sentenza che definisce il giudizio non è appellabile e ricorre per lo più una disposizione eccezionale per il nostro ordinamento: il Giudice ordinario può sospendere il provvedimento e prescrivere l'adizione di misure ritenute necessarie all'Amministrazione titolare o responsabile dei dati (nonché condannare al risarcimento dei danni) e ciò "anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E)". È pacifico, quindi, che il Giudice civile possa in quest'ipotesi annullare/riformare il provvedimento amministrativo.
Se queste peculiarità hanno superato, con un tratto di penna, ampi dibattiti dottrinali, i limiti contenuti nella legge delega per l'attuazione del GDPR non hanno consentito al legislatore delegato di superare un'aporia sistematica che appare evidente da un confronto di diritto comparato.
Il capo V della legge 7 agosto 1990 n. 241, che contiene le disposizioni generali sul procedimento amministrativo, è dedicato al diritto di accesso dell'interessato (mediante presa visione e estrazione di copia) di documenti amministrativi.
Questi documenti possono contenere dati personali propri del soggetto interessato ovvero di soggetti terzi. In entrambi i casi, possono entrare in conflitto le competenze dell'Amministrazione a cui viene rivolta l'istanza di accesso (ovvero del Difensore civico ex art. 25 legge 241/1990 o della

Commissione per l'accesso ai documenti amministrativi, incardinata presso la Presidenza del Consiglio dei Ministri ex art. 27 legge 241/1990), con le competenze dell'Autorità Garante della Tutela dei dati personali.
Laddove accada, il comma 4 dell'art. 25 della legge 241/1990, nel testo risultante da una serie di modifiche, prevede queste forme di raccordo: "Se l'accesso è negato o differito per motivi inerenti ai dati personali che si riferiscono a soggetti terzi, la Commissione provvede, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta, decorso inutilmente il quale il parere si intende reso. Qualora un procedimento di cui alla sezione III del capo I del titolo I della parte III del decreto legislativo 30 giugno 2003, n. 196, o di cui agli articoli 154, 157, 158, 159 e 160 del medesimo decreto legislativo n. 196 del 2003, relativo al trattamento pubblico di dati personali da parte di una pubblica amministrazione, interessi l'accesso ai documenti amministrativi, il Garante per la protezione dei dati personali chiede il parere, obbligatorio e non vincolante, della Commissione per l'accesso ai documenti amministrativi. La richiesta di parere sospende il termine per la pronuncia del Garante sino all'acquisizione del parere, e comunque per non oltre quindici giorni. Decorso inutilmente detto termine, il Garante adotta la propria decisione".
Se in qualche misura il problema può ritenersi così risolto nella fase amministrativa/procedimentale, esso persiste in ambito giurisdizionale.
In caso di diniego di accesso agli atti amministrativi, infatti, l'interessato può promuovere ricorso giurisdizionale. Sennonché la scelta operata dal legislatore in questo caso è quella opposta a quella sopra indicata: queste controversie sono attribuite alla giurisdizione esclusiva del Giudice amministrativo (cfr. art. 116 del D. lgs. 2 luglio 2010 n. 104, Codice del processo amministrativo).
Può quindi capitare che, mentre il Giudice amministrativo sta decidendo se sia o meno corretto il provvedimento di un Ente pubblico che neghi l'accesso alla documentazione amministrativa, il soggetto dei cui dati si discute (il controinteressato nel ricorso davanti al Tribunale amministrativo regionale) promuova un parallelo ricorso avanti al Giudice ordinario per ottenere la rettifica o la cancellazione dei dati stessi.
Le due Autorità giurisdizionali potrebbero decidere in modo difforme e, dal momento che eccezionalmente entrambe hanno facoltà di impartire ordini all'Amministrazione, quest'ultima potrebbe vedersi rivolgere indicazioni opposte.

Prof. Avv. Alessandro Dario Cortesi
Professore a contratto di informatica giuridica
Università Cattolica del Sacro Cuore Milano
Facoltà di Giurisprudenza