Alla ricerca dei dati perduti

Emilio Girino
Avvocato in Milano - Managing Partner, Studio Ghidini, Girino & Associati - Docente CUOA Finance - già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Franco Estrangeros
Avvocato in Milano - Partner, Studio Ghidini, Girino & Associati - già Membro dell'Arbitro Bancario Finanziario (Collegio di Milano e Collegio di Coordinamento)

Avrebbero potuto analizzare e mettere su carta,
nei minimi particolari, tutto quello che
s'era fatto, s'era detto e s'era pensato

(George Orwell, *Millenovecentottantaquattro*, Londra, 1948)

1. Il dato personale fra rivelazione e fraintesi

Correva l'anno 1997. Partecipammo ad uno dei primi convegni che promettevano di svelare ogni segreto della neonata legge del 13 dicembre 1996, n. 675[1]. Ne uscimmo molto perplessi.

Tra sfoggi di sapienza precoce, convinta preveggenza e immancabili, interessati sussurri di terrorismo normativo prossimo venturo, presto l'atmosfera si fece greve. Nella pausa caffè un allora giovane procuratore legale ci consegnò il suo biglietto da visita e, fra il serio e il faceto, dichiarò che con quel gesto autorizzava il trattamento dei suoi dati anche per l'invio degli auguri natalizi chiedendoci eguale liberatoria quando ricambiammo porgendogli le nostre carte. Un noto avvocato di mezza età, l'occhio illividito

[1] "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" in G.U. 8 gennaio 1997, n. 5., S.O.

dallo scandalo, chiosò le prime relazioni parlando di "situazione carceraria". Due funzionari bancari cominciarono fibrillanti a stilare una rozza lista di adempimenti sul tovagliolo di carta per cappuccino, nel frattempo litigando animatamente. Un brillante consulente, attratto dalla problematica dei dati sessuali, dopo aver premesso che si poteva essere eccellenti professionisti pur concedendo a pagamento le proprie grazie, si domandò cosa sarebbe successo se suoi altrettanto brillanti colleghi o colleghe si fossero dedicati, a tempo perso, alla così chiamata pratica più antica del mondo e se il dato relativo alla loro seconda e segreta occupazione fosse divenuto di pubblico dominio. Vi fu anche chi, con un ardito accostamento fra privacy e responsabilità del produttore, concluse che i fastidi della prima si sarebbero risolti con gli stessi metodi usati per scansare quelli della seconda: una solida polizza assicurativa. Le agendine, allora per lo più cartacee, che tenevamo nelle borse o nella tasca interna della giacca, affollate di nomi, indirizzi e numeri telefonici, parevano improvvisamente essere divenute armi improprie. Sotto il ventaglio di questi variopinti commenti, timori che si tramutavano in allucinazioni legali, battute che soffocavano ansie private, iperboli da follia collettiva, si celava, inespressa ma nitida, la convinzione che il dato personale fosse nato insieme alla legge partorita per regolarlo, quasi per un bizzarro fenomeno di partenogenesi: la legge che protegge i dati è pur anche quella che li crea.

Niente di più assurdo. Da qui la nostra perplessità. I dati personali esistono da sempre, da quando cioè l'essere umano ha iniziato a convivere socialmente con i suoi simili e nell'ordinamento moderno non mancavano, ben prima della L. 675/1996, né mancano ora fior di norme volte a proteggerli. Basti pensare alla disciplina codicistica della tutela del nome, al divieto di intercettazioni illegali, al reato di intrusione nella vita privata con mezzi di riproduzione a distanza, al reato di sostituzione di persona; o ancora, più semplicemente, alla diffamazione che crimine resta anche quando i fatti che essa propala sono veri[2]: presidi legislativi posti a tutela di informazioni di vario genere che riguardano gli individui.

Del resto che cos'è un dato personale se non un'informazione su una persona? Azzardando una categorizzazione, si potrebbe concludere che il dato personale corrisponde a cinque ideali domande che un individuo può porsi riguardo ad un altro: chi è, come sta, cosa possiede, cosa pensa, cosa fa, domande cui corrispondono, rispettivamente, altrettante tipologie di informazioni, ossia

[2] La tutela dei dati, d'altronde, era già nel preciso mirino del legislatore comunitario a seguito della Convenzione di Strasburgo n. 108/1981, antesignana e ava della disciplina in parola (v. par. 2).

(a) identità personale; (b) condizioni sanitarie; (c) disponibilità economiche; (d) opinioni o appartenenze politiche, filosofiche o religiose; (e) costumi di vita privata. Esulano dal concetto di dato personale, quanto meno di dato personale proteggibile per legge, esulano cioè dalla corrispondente domanda "cosa fa?" le informazioni sull'attività professionale svolta da un individuo e ciò per la buona ragione che l'esercizio di un'attività a scopo economico implica un'interazione individuale tale da escludere necessariamente la pretesa di riservatezza sul fatto in sé di svolgere quella data attività.

L'area di protezione delle informazioni a sua volta si contrae, spesso sensibilmente quando non totalmente, in ragione dell'uso che il singolo individuo fa dei propri dati. Si può essere convinti fedeli o irriducibili atei ma, se pubblicamente lo si professa, sarà impossibile proibire a terzi di impiegare quel dato nel rapportarsi *a* noi o nel rapportarsi ad altri terzi *su* di noi. Possiamo rifiutarci di fornire il nostro nome e cognome al primo passante che ce lo domandi, ma se abbiamo aperto un profilo su un social network sarebbe semplicemente demenziale pretendere riservatezza sulla nostra identità. Vi sono poi atti quotidiani, prevalentemente negoziali, che inevitabilmente implicano l'abdicazione alla segretezza: un contratto di lavoro, l'acquisto di un'automobile, la stipulazione di un mutuo, l'abbonamento ad un periodico sono solo alcuni ordinari esempi di come la nostra pretesa di riservatezza debba, per forza di cose, cedere il posto alla soddisfazione delle nostre necessità.

Il perimetro protettivo si restringe ancor più sensibilmente nel momento in cui l'individuo interagisce con un ente pubblico o con le autorità di pubblica sicurezza e giustizia. Se possiamo rifiutare di esibire la nostra patente al primo che capita, non possiamo fare altrettanto ad un blocco di polizia stradale. Chiamati a testimoniare in un processo e interrogati su che cosa stessimo facendo in una data circostanza, non possiamo esimerci dal dirlo e soprattutto dal dire il vero. L'amministrazione tributaria può legittimamente controllare i nostri conti bancari. Altrettanto legittimamente le nostre cartelle cliniche riposano negli archivi del servizio sanitario pubblico.

Quest'ultimo rilievo, in apparenza banale, diviene invece un'essenziale chiave di lettura dell'impianto normativo della riservatezza che opera, nei limiti in cui opera, solo nel rapporto fra soggetti privati, mentre risulta fortemente affievolita, se non del tutto azzerata, nei confronti di istituzioni o autorità superindividuali (torneremo oltre e più approfonditamente sul punto: *infra* parr. 7-8).

Accanto a coloro che incapparono nell'equivoco per cui sarebbe stata la L. 675 a "creare" la nozione giuridica di dato, vi furono anche coloro che salutarono quella legge con un grido liberatorio, illudendosi che con essa

ciascun individuo avrebbe potuto finalmente racchiudere la propria esistenza dentro un impenetrabile scrigno. Se la prima lettura, oltre a essere erronea, era anche illogica, la seconda era semplicemente ingenua. La vera funzione della legge in parola non consisteva nella criptazione blindata dei dati personali, bensì nell'affermazione della *proprietà individuale* del dato, assicurando diversi livelli di protezione di quell'*asset* nel rapporto fra privati, lasciando al proprietario la libertà di un uso cosciente del dato medesimo, escludendo o minimizzando quella libertà nel rapporto con la realtà pubblica e istituzionale. La funzione della legge non mirava, quindi, al rafforzamento della riservatezza, bensì alla "legalizzazione privatistica" dei dati personali.

2. Alle origini della normazione: la prospettiva della digitalizzazione e lo "spossessamento" naturale del dato personale. L'esigenza di protezione

Solo in pochi virtuosi casi il diritto e l'attività normativa sono riusciti ad anticipare le esigenze sociali determinate dall'evoluzione di mezzi e strumenti e del relativo mercato in cui gli stessi si adoperano o che gli stessi creano. Nel caso di specie la nuova normativa, se non del tutto anticipatoria rispetto alla rivoluzione digitale esplosa nel nuovo millennio, ha posto le basi per affrontare gli effetti della globalizzazione delle reti e dei canali di comunicazione.

Già allora, negli anni '90, si era ben consapevoli dei probabili esiti della digitalizzazione e di come la sua diffusione, guidata dall'alluvionale e indistinguibile esercito degli internauti, avrebbe consentito, nel volgere di pochi anni, una circolazione potenzialmente illimitata nel tempo, nella qualità e nella quantità, di informazioni e dati. Erano i tempi del web 1.0 e delle vetrine on line, dei portali informativi e dei primi siti di commercio elettronico rapidamente disciplinati dalla Direttiva 2000/31 CE[3]. Le e-mail avevano già quasi pensionato il vecchio telefax e il nostro vivere quotidiano (anche professionale) era già sovvertito. Da lì a breve si sarebbe assistito alla detonazione dei blog, dei social network e dei portali di contenuti attraverso i quali le informazioni personali, proprie o di terzi, avrebbero potuto, nel volgere di un attimo, essere rese pubbliche e affidate alla memoria indelebile della rete.

Il mondo occidentale, in particolare quello europeo, era inoltre percorso

[3] Dir. 8 giugno 2000 n. 2000/31/CE "Relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno" in G.U.C.E. 17 luglio 2000, n. L 178.

da un mutamento epocale. Nel 1992, con la sottoscrizione del Trattato di Maastricht si erano fissate le regole politiche e i parametri economici e sociali necessari per l'effettiva integrazione europea e per la formazione del Mercato Unico, con l'abbattimento delle dogane fra Stati intervenuto il 1° novembre 1993. Per ottimizzare gli effetti della libera circolazione di merci, persone, servizi e capitali diveniva inevitabile limitare le disomogeneità nelle normative nazionali disciplinanti l'uso dei dati personali connessi agli scambi, normative che almeno alcuni Stati si erano già dati[4].

Nella prospettiva della rivoluzione digitale, nel contesto storico, economico e politico dianzi accennato e a seguito di estenuanti trattative in ambito europeo, nell'ottobre del 1995 venne pubblicata la Direttiva 95/46 CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati[5]. Con quest'ultima il legislatore comunitario, nel contesto evolutivo del mercato digitalizzato ormai alle porte e per finalità intrinseche alla creazione del Mercato Unico Europeo, riprese e sviluppò, con propositi di armonizzazione, i principi già noti in ambito europeo e portati dalla Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981 dal Consiglio d'Europa a salvaguardia dei "*diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano*"[6]. Il primo ad adeguarsi fu proprio lo Stato italiano emanando

[4] Cfr. Considerando nn. 3 e 5 della Dir. 24 ottobre 1995 n. 95/46 CE in G.U.C.E. 23 novembre 1995, N.I. 281/31 secondo cui " (3) considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'art. 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali delle persone"; (5) "considerando che l'integrazione economica e sociale derivante dall'instaurazione e dal funzionamento del mercato interno ai sensi dell'articolo 7 A del trattato comporterà necessariamente un sensibile aumento dei flussi transfrontalieri di dati personali tra tutti i soggetti della vita economica e sociale degli Stati membri, siano essi privati o pubblici; che lo scambio di dati personali tra imprese stabilite i Stati membri differenti è destinato ad aumentare; che le amministrazioni nazionali dei vari Stati membri debbono collaborare, in applicazione del diritto comunitario, e scambiarsi i dati personali per poter svolgere la loro funzione o esercitare compiti per conto di un'amministrazione di un altro Stato membro, nell'ambito dello spazio senza frontiere costituito dal mercato interno".

[5] In G.U.C.E. 23 novembre 1995, L 281/31.

[6] Nella quale, all'art. 1 già si proclamava in favore delle persone fisiche il "diritto alla vita privata nei confronti dell'elaborazione automatizzata dei dati di carattere personale" e, all'art. 4, si raccomandava ad ogni Stato partecipante l'adozione nel proprio diritto interno delle "misure necessarie per dare effetto ai principi fondamentali per la protezione dei dati enunciati nel presente capitolo": dunque, come enunciato al successivo articolo 5, si imponeva che i "dati di carattere personale oggetto di un'elaborazione automatizzata" fossero: "a) ottenuti e elaborati in modo lecito e corretto; b) registrati per scopi determinati e legittimi ed impiegati in una

nel dicembre dell'anno successivo la L. 675/1996 e così attuando i precetti comunitari secondo un approccio estensivo, non rinunciando cioè ad ampliare portata e ambiti applicativi delle linee regolamentari europee che all'epoca non precludevano scelte interne più tutelanti (v. *amplius* par. 3).

L'introduzione della disciplina sulla protezione dei dati personali ebbe indubbiamente un impatto rilevante. Al di là dei luoghi comuni e dei fraintendimenti applicativi iniziali (come rammentato nel par. 1), la *ratio* innovatrice era evidente: la norma non s'occupava di rafforzare direttamente il diritto alla riservatezza delle persone (della loro vita privata e familiare, del loro domicilio, delle loro comunicazioni); altre e anteriori norme, si è dianzi notato, già se ne facevano carico. L'impianto legislativo era invece volto a riconoscere agli interessati una protezione qualificata, disciplinando la fase del rilascio del dato e quella della sua circolazione e assoggettando i trattamenti dei dati personali a presupposti di liceità e di specifica e informata autorizzazione dell'interessato. In quest'ambito, in capo agli operatori che trattavano dati personali di terzi, s'introducevano standard di sicurezza e obblighi di informazione preventiva, vietando il trasferimento dei dati personali in quei Paesi extra UE che non garantissero la soddisfazione degli standard minimi di protezione previsti dalla disciplina europea.

Non s'intendeva cioè rabbuiare una stanza illuminata semplicemente spegnendo la luce (così figurativamente rappresentando il diritto alla riservatezza), ma contribuire al conseguimento della riservatezza canalizzando i raggi di luce provenienti dalla fonte luminosa (così figurativamente rappresentando la circolazione dei dati personali). Il tutto non già vincolando l'interessato alla riservatezza, ma semplicemente mettendo nelle sue mani gli strumenti per limitare la circolazione dei propri dati personali: è l'interessato che può inibire ovvero limitare la circolazione dei dati, ovvero, renderli pubblici.

Si volle cioè attribuire autonoma rilevanza al diritto delle persone di evitare che soggetti terzi raccogliessero e/o utilizzassero informazioni riferite ai primi, senza il loro consenso o senza una specifica previsione di legge, rimanendo invece escluso da tale disciplina il diritto alla riservatezza, inteso

maniera non incompatibile con detti fini; c) adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati; d) esatti e, se necessario, aggiornati; e) conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati". All'art. 6 già si individuavano "*Categorie speciali di dati*" con specifico riferimento a quelle idonee a rivelare "l'origine razziale, le opinioni politiche, le convinzioni religiosi o altri credo … lo stato di salute e … la vita sessuale". Per tali dati la norma prevedeva il divieto di "essere elaborati automaticamente a meno che il diritto interno non preveda garanzie adatte".

come diritto di escludere altri dalla propria vita privata[7]. La L. 675/1996, insomma, affermava precisamente la proprietà del dato in una logica e in una prospettiva essenzialmente privatistica.

3. L'approccio normativo iniziale. L'estensione della tutela alle persone giuridiche. La preminenza del taglio formale: il tormentone del consenso e della notificazione dei trattamenti. L'organizzazione aziendale

Rispetto agli intendimenti espressi nella Direttiva 95/46, il testo attuativo di cui alla L. 675/1996 si rivelò più complesso e articolato e colpì per la portata estensiva della disciplina rispetto ai dettami desumibili dalla norma europea. Il legislatore italiano estese le prerogative di tutela riferita ai dati personali anche alle persone giuridiche[8] con ciò elevando a dismisura la portata degli incombenti volti a garantire il rispetto delle prescrizioni[9]. Estensione doppiamente impropria rispetto alle finalità di tutela della nuova disciplina. Una prima volta perché risulta francamente poco condivisibile (in quanto non funzionale) il riconoscimento di un diritto alla riservatezza in capo ad un soggetto (persona giuridica) al quale assai difficilmente può essere attribuito un interesse alla privacy assimilabile a quello di una persona fisica (la persona giuridica è, per sua natura e in senso lato, "pubblica" nel senso che è votata per definizione a rendere disponibili i suoi dati e la sua stessa identità ai terzi con cui interagisce). Una seconda volta perché la tutela delle informazioni riservate per gli operatori commerciali era, già all'epoca, oggetto di protezione ai sensi dell'art. 6-bis del R.D. 29 giugno 1939, n. 1127 e lo è tutt'oggi, peraltro in termini ulteriormente rafforzati, ai sensi degli artt. 98 e ss. del D.Lgs. 10 febbraio 2005, n. 30 (Codice della proprietà industriale). Tra le definizioni iniziali del testo normativo, si rinvenne, a sorpresa, anche quella di "banca dati" che innescò, almeno in sede di prima applicazione,

[7] Al paragrafo 1.12 della Relazione 1997 del 30 aprile 1998, il Garante Privacy espressamente osservava come "Per effetto della legge n. 675/1996, che si pone come disciplina generale sul trattamento dei dati personali, il diritto alla riservatezza assume connotati del tutto nuovi rispetto all´originario nucleo del 'diritto ad essere lasciato solo', definito in via prevalentemente giurisprudenziale e solo nell´ambito di alcuni settori, come quello dell'attività giornalistica o dell´attività di impresa". Per un riferimento puntuale alla "teoria del diritto di solitudine" concepito nell'Inghilterra vittoriana v. S. Rodotà, *Privacy, libertà, dignità* in *Privacy.it*, 2.

[8] L'art. 1 comma 2°, lett. c) della legge in parola riferiva il "dato personale" espressamente a "*qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione…*"

[9] Posto che gli incombenti derivanti dall'applicazione della legge dovevano applicarsi non solo nei confronti della clientela ma anche nei rapporti commerciali, tra società, al fine del trattamento dei relativi dati, sostanzialmente identificativi, di contatto e fiscali.

un acceso dibattito sulla rilevanza, ai fini del riconoscimento della tutela della L. 675/1996, dell'inserimento, o meno, dei dati personali in banche dati organizzate[10]. In realtà, da una semplice lettura del testo normativo, risultava sin da allora evidente come l'unico effetto desumibile dal fatto che il dato fosse o meno inserito in banche dati potesse rilevare ai soli fini della notifica al Garante (ai sensi dell'art. 7, comma 4°, lett. g) L. cit.), non influendo per nulla sull'applicazione delle tutele previste dalla disciplina in parola[11].

Il semi-equivoco in cui incorsero i primi commentatori consisteva nel ritenere che la protezione del dato dipendesse dal suo inserimento in un sistema organizzato: non qualunque dato è tutelato ma solo quello che confluisce in una banca dati o in un comunque allestito archivio. Parliamo di semi-equivoco perché, mentre la proposizione che precede era totalmente errata e smentita dal dato normativo testuale, in realtà nella legge era rinvenibile, sia pur *a contrariis*, una pre-condizione di tutela. Tutto risiedeva nell'art. 3 il quale escludeva l'applicazione della disciplina nel solo caso di dati raccolti per fini esclusivamente privati (l'agendina personale per intenderci[12]), così decretandone invece l'applicazione per ogni altro fine, dunque essenzialmente per fini economici, istituzionali, associativi. La precondizione non era dunque il *dove* il dato sarebbe stato stoccato ma il *fine* per il quale il ricevente lo avrebbe utilizzato. Con un'unica eccezione all'eccezione: l'applicazione, anche nel caso di trattamento a puro fine privato, delle misure di sicurezza (v. *infra*). Anche in questo senso la legge guardava avanti e pensava, più che al surreale e agevolmente scassinabile lucchetto sulle agende cartacee, al proliferare degli apparati mobili sui quali sarebbero confluiti, come poi confluiranno in massa, miriadi di indirizzi, numeri, messaggi e immagini di terzi: dunque ai sistemi di criptazione che oggi permettono di oscurare quei dati per scelta dell'utente oppure ove lo *smartphone* vada smarrito. Pur

[10] Cfr. art. 1, comma 2° lett. a) della legge in parola che definiva "banca dati" come "qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento".

[11] Successivamente, con le modifiche apportate alla L. 675/1996 dall'art. 1 del D.Lgs. 28 luglio 1997. n. 181, la rilevanza della mancata registrazione dei dati personali trattati in una banca dati si risolveva nella possibilità di dar corso ad una notifica al Garante dei trattamenti in forma semplificata (art. 7 co. 5 bis lett. c) della L. 675/1996.

[12] Peraltro con un mai (volutamente) affrontato né risolto problema: come deve essere trattata, ad esempio, l'agenda personale d'un professionista in cui confluiscono sia i dati di parenti e amici sia quelli di aziende, clienti e altri soggetti che quell'agenda permetterà di rintracciare per fini non privati? Problema volutamente ignorato e irrisolto perché obiettivamente irrisolvibile se non a patto di condannare realmente la circolazione dei dati fra privati o alla violazione perenne e impunita o all'ingabbiamento paralizzante.

approssimativa sul punto, la normativa avvalorava la sua vocazione divinatoria su quelle che sarebbero state, nel breve e medio termine, le evoluzioni (o involuzioni) di un sistema nel quale i dati sarebbero stati sempre più inevitabilmente fragili perché sempre più facilmente aggredibili.
Al di là degli indiscussi meriti sintetizzati nel principio di proprietà sopra richiamato, la L. 675/1996 si connotò per un elevato tasso di "burocratizzazione", caratterizzato da formalismi sproporzionati e inutili.
Con riferimento, ad esempio, al cennato istituto della notifica al Garante, almeno in prima battuta, l'incombente venne sostanzialmente imposto, senza esclusioni (tranne quella poc'anzi evocata), a tutti i soggetti che operassero i trattamenti di dati personali (cioè a tutte le persone fisiche e/o giuridiche che, nello svolgimento della propria attività, utilizzassero dati personali di terzi, quindi anche alle piccole realtà che operavano trattamenti ordinari e non significativi) implicando un onere tanto rilevante e costoso per gli operatori quanto di poca o nulla utilità al fine dell'esercizio dei controlli. Il principio è ben noto: troppe informazioni, nessuna informazione (più o meno come nel distopico, e come tale preveggente, *Brazil* di Terry Gilliam, dove l'ipertrofia informativa obbliga il Ministero dell'Informazione ad istituire un apposito Reparto Recupero Informazioni, in cui il protagonista cercherà d'intrufolarsi per rintracciare la sua amata compagna di rivolta).
Alla notificazione al Garante dei trattamenti s'aggiungeva la predisposizione delle informative privacy destinate agli interessati dei trattamenti, informative che si ponevano alla base del consenso specifico e informato che l'interessato avrebbe dovuto rilasciare. Il problema fu che, in considerazione della quantità e della qualità delle informazioni che dovevano essere contenute nelle informative, al di là di pochi scrupolosi e meritevoli operatori, le stesse si ridussero di fatto a prestampati fra loro similari, ridondanti e ripetitivi. Le informative non venivano nella realtà lette dagli interessati e il consenso ai trattamenti si risolveva in una pre-compilazione del modulo da parte del titolare, con apposizione di una firma sostanzialmente "in bianco".
Tanto generò altresì una sorta di schizofrenia operativa che conduceva a richiedere il consenso anche in quei casi e per quei fini nei quali e per i quali la legge stessa non richiedeva alcun consenso, in quanto implicito nella volontà insita nel gesto stesso di avvio della relazione interpersonale. Quello del consenso fu una specie di tedioso tormentone che spesso distolse gli operatori dall'osservanza delle restanti disposizioni della legge, nel più che erroneo convincimento che il vero problema fosse far firmare l'annuente pezzo di carta: un tormentone proseguito sino ai giorni attuali (o almeno sino alla revisione indotta dall'intervenuta entrata in vigore del GDPR: cfr. par. 6) ove, o per inerzia degli obbligati o per dato-fobia indotta, spesso

abbiamo visto informative privacy richiedenti ossessivamente consensi superflui e non imposti da alcuna norma.
Per il resto, una rilevante parte della L. 675/1996 era dedicata ad imporre a ciascun titolare un'organizzazione aziendale interna volta a garantire il, e a responsabilizzare le funzioni dedicate al, rispetto della corretta esecuzione dei trattamenti. Nacquero allora le figure del "titolare" e del "responsabile" dei trattamenti e i dipendenti o collaboratori che materialmente operavano il trattamento dei dati nell'esercizio delle proprie funzioni, dovevano essere a ciò "incaricati" dal "titolare" o dal "responsabile"[13]. E fu sempre la L. 675/1996 ad introdurre le già menzionate misure minime di sicurezza, prevedendo in ogni caso che l'organizzazione degli strumenti deputati al trattamento dei dati personali di terzi fosse adeguata al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l´adozione di idonei e preventivi accorgimenti tecnici, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta[14]. Si comincerà dagli armadi di ferro chiusi a chiave per arrivare alle password, ai firewall e ad altre consimili barriere.

4. L'evoluzione della L. 675/1996. Il ruolo del Garante Privacy. Il Codice Privacy

Conclusa la fase di rodaggio, apportati numerosi correttivi funzionali volti alla semplificazione, pubblicati i molteplici regolamenti attuativi, già nei primi anni del nuovo millennio la disciplina sulla privacy assumeva contorni operativi più ragionevoli e definiti.
Nel 1997, con due diversi decreti legislativi[15] si ammise la forma orale per l'informativa all'interessato (anche se si ribadì che la prestazione del consenso – se necessaria – dovesse essere comunque provata per iscritto), si introdusse l'informativa semplificata agli interessati nonché i casi di notifica semplificata al Garante e di esenzione dalla stessa (esenzione che poi, nel 2011, venne ulteriormente ampliata prevedendone l'obbligatorietà per i soli trattamenti che, per le modalità o per la natura degli interessati, fossero suscettibili di recare pregiudizio ai diritti e alle libertà dei medesimi)[16].

[13] Cfr. artt. 1, comma 2°, lett. d) ed e) e 8 della L. 675/1996.
[14] Cfr. art. 15 della L. 675/1996 .
[15] Ci riferiamo al D. Lgs. 9 maggio 1997, n. 123 in G.U. 10 maggio 1997 n. 107 (art. 1) e al D.Lgs. 28 luglio 1997, n. 255 in G.U. 5 agosto 1997, n. 181 (art. 1).
[16] Con D. Lgs. 28 dicembre 2001, n. 467 (Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali, a norma dell'articolo 1 della L. 24 marzo 2001, n.

Con il D.P.R. 318/1998 vennero pubblicate le norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali[17]. Nel 2001 si semplificò la comunicazione dei dati personali dell'interessato escludendone il consenso qualora ciò fosse necessario per l'esecuzione di un contratto o di obblighi precontrattuali ovvero quando la comunicazione di tali dati venisse svolta sulla base di un legittimo interesse del titolare ma non a danno delle libertà fondamentali dell'interessato o di un suo legittimo interesse[18] (principio già ovviamente desumibile dal testo originario ma la cui chiarificazione non bastò, tuttavia, come s'è detto, a sgonfiare il tormentone consensualista). Con lo stesso provvedimento legislativo, soprattutto, si attribuì al Garante Privacy l'obbligo di emanazione di codici di deontologia e di buona condotta da adottarsi entro il giugno 2002 in alcune specifiche materie[19], codici che risolsero, nei singoli settori sopra menzionati, numerosissimi dubbi applicativi.

Nel 2003 la privacy ebbe il suo codice. Abrogandola, il Codice Privacy[20] riproponeva i contenuti della L. 675/1996 inserendo, quale "testo unico", le discipline, anche regolamentari, ad essa inerenti. Ma il *restyling* e il progresso normativo non si fermarono qui.

In attuazione della Direttiva 2002/58[21], venne introdotta la disciplina in materia di "Comunicazioni elettroniche". Un provvedimento che non passò inosservato ma che non ricevette l'onòre di essere riconosciuto come un vero punto di svolta, come il passaggio cioè da un modello di regolamentazione

127) in G.U. 16 gennaio 2002, n. 13.

[17] D.P.R. 28 luglio 1998, n.318, Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996.

[18] Cfr. art. 12, comma 1 lett. b) e lett. h-bis siccome, rispettivamente, modificata e introdotta dall'art. 5 del D. Lgs. 467/2001.

[19] Le materie oggetto di disciplina tramite l'emissione dei codici di deontologia e di buona condotta da parte del Garante Privacy furono le seguenti: trattamenti eseguiti da fornitori di servizi di comunicazione e informazione; necessari per finalità previdenziali o per la gestione del rapporto di lavoro; effettuati a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva; svolti a fini di informazione commerciale; effettuati nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati; effettuati con strumenti automatizzati di rilevazione di immagini.

[20] Il D. Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) in G.U. 29 luglio 2003, n. 174

[21] Dir. 12 luglio 2002, n. 2002/58/CE (Direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche) in G.U.C.E. 31 luglio 2002, n. L 201, attuata con L. 3 febbraio 2003, n. 14 (legge comunitaria 2002) e con L. 31 ottobre 2003, n. 306 (legge comunitaria 2003).

formalistico e generalista ad un progetto di progressivo spostamento del baricentro normativo alla protezione specifica e sostanziale del dato. La disciplina, infatti, introduceva regole sulla raccolta di dati dell'abbonato o dell'utente, disciplinava la raccolta di dati relativi al traffico, le modalità di comunicazione della fatturazione dettagliata dei servizi, la sottoposizione a consenso dell'interessato dei trattamenti del dato relativo all'ubicazione (cioè la posizione geografica del terminale dell'utente), le regole per l'esecuzione delle comunicazioni indesiderate. Il salto qualitativo è innegabile: dalla semplice regolamentazione della cessione del dato si passa ad una protezione oggettiva o, se vogliamo, ad un ripensamento del dato in sé. La specificità della disciplina è tale per cui, indipendentemente dalle scelte dell'interessato, il dato va comunque trattato in un certo modo, con certe cautele, entro certi limiti, con certi accorgimenti: modi, cautele, limiti e accorgimenti che si applicano in modo oggettivo, senza specifici vincoli di forma ma con obbligo di risultato sostanziale.

Nell'evoluzione della disciplina italiana sulla protezione dei dati personali, merita poi rammentare, finalmente nel 2011, l'attesa e opportuna cancellazione dalla definizione "dati personali" del riferimento alle "persone giuridiche, enti e associazioni"[22]. Anche il nostro legislatore, in coerenza con la scelta espressa sin dall'originaria Direttiva 95/46, riconobbe il primato di protezione dei dati personali riferibili alle persone fisiche, rispetto a quella delle persone giuridiche, il ché comportò una coerente semplificazione, quantomeno, nelle relazioni fra imprese ed enti (pur se, a tutt'oggi, al pari del consenso, non è raro vedere includere clausole *privacy* nei contratti fra società).

Nel mentre la normativa primaria s'affinava, semplificandosi e adattandosi al mutare del circostante, il Garante Privacy non stette come il savio cinese sulla riva del fiume. In quegli stessi anni assistemmo ad una ponderosa azione d'indirizzo da parte dell'Autorità che, oltre allo svolgimento della vigilanza ordinaria, emanò numerosi provvedimenti interpretativi e/o prescrittivi per chiarire varie tematiche: dalla tracciabilità delle operazioni bancarie alla circolazione dei dati nei gruppi bancari, dagli obblighi riferibili all'utilizzo dei sistemi di informazione creditizia all'amministrazione dei condomini, dall'utilizzo di *cookies* in internet (torneremo oltre sul punto: par. 8) ai *social media*, dal marketing diretto al marketing telefonico. Nuovamente la cifra settoriale e sostanzialistica, che aveva ispirato la Direttiva sulle comunicazioni elettroniche, si riafferma imprimendo alla disciplina un taglio più impositivo e più sottratto alla mera negoziazione privata (sia pur entro certi limiti sui

[22] Avvenuta per effetto dell'art. 40, comma 2, lett. a), D.L. 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla L. 22 dicembre 2011, n. 214

quali torneremo e che rappresentano il vero tallone d'Achille dell'architettura normativa e regolamentare).
Malgrado le semplificazioni, il confezionamento di un testo unico, la cancellazione della deviante equiparazione fra dati degli individui e dati degli enti, l'avvio di un percorso sostanzialistico e le suddette azioni d'indirizzo del Garante, per il resto l'impianto della normativa rimase fondamentalmente immutato: informativa, consenso esplicito salvo deroghe espressamente previste, diritto di accesso, modifica e cancellazione dei dati trattati; titolare, responsabile e incaricati del trattamento; specifici presidi tecnici di sicurezza. Il tutto in relazione all'operatività sia dei privati sia degli enti pubblici. In quest'ambito, un differente grado di protezione veniva riservato ai dati "sensibili" ovvero ai dati "giudiziari". Ma nulla più.

5. L'esplosione della tecnologia invasiva, il fenomeno dei Big Data e la pericolosità sociale dell'*Internet of Things*

Nel nuovo millennio si realizza in pieno e in tempi rapidissimi ciò che nel corso degli anni '90 si era ben intuito sarebbe successo. Dall'era web 1.0 (racchiusa all'incirca nell'ultimo decennio del Novecento), si passò velocemente all'era web 2.0 contraddistinta dalla possibilità degli utenti internet di interagire con i siti web degli operatori, introducendo a loro volta contenuti. Si registrò il boom dei *social media* e dei *blog* e una crescita esponenziale degli stessi portali di condivisione di contenuti quali *YouTube* e *Wiki*. Senza contare tutti i servizi resi accessibili dagli operatori web e di cui si dotò anche l'amministrazione pubblica (l'amministrazione digitale, la sanità digitale, il processo civile telematico, solo per citare le casistiche più dirompenti).
Ben presto, col progredire tecnico degli *smartphone* e delle *app* (applicazioni che consentono agli utenti di giovarsi di svariati servizi, dal semplice gioco ai servizi bancari, ai servizi di investimento e assicurativi, ai servizi delle pubbliche amministrazioni, a servizi con finalità di monitoraggio del sonno, dell'attività sportiva, della gestione del tempo, in generale), nonché con la fornitura di sistemi di memorizzazione *in cloud*, s'inaugura l'era web 3.0. Internet diventa un database universale in evoluzione continua e incontrollata, capace d'incidere prepotentemente, invasivamente ed anche, sia permesso, arrogantemente sui comportamenti sociali (chiamasi in gergo, "Web Potenziato"). Si sostiene cioè, del tutto condivisibilmente, che in forza dell'interazione diretta consentita da internet tra azienda/consumatore, politico/elettore, artista/fan, si sviluppino *on line* attraverso i social network (pseudo) relazioni atte a incidere sulle scelte e sui comportamenti delle

persone, relazioni ed effetti che, in precedenza – per intensità, velocità e potenza del mezzo – non erano ipotizzabili[23].

Per quanto l'era digitale sia sempre in costante e inarrestabile evoluzione (già si parla di Web 4.0, contraddistinto dalla possibilità di configurare in rete un *alter ego* digitale per ciascun utente, in considerazione del volume di informazioni riferibili appunto agli utenti che vengono immesse in rete), ciò che qui rileva è la massa di dati che l'evoluzione digitale, grazie a server e sistemi di trattamento digitale automatizzato e da elaboratori sempre più potenti, consente di raccogliere, conservare, analizzare, confrontare. Massa di dati che consente, per ciascun utente, grazie all'attività di selezione, comparazione e profilazione, la creazione di ulteriori dati e informazioni riferibili a ciascun individuo.

È in definitiva il tema dei Big Data. Nient'altro che insiemi di dati riferibili ad un individuo o a un gruppo di individui per effetto di una correlazione c.d. interferenziale fra tipologie di informazioni di natura e origine diversa. Correlare e incrociare dati fisici o fisiognomici, professionali, finanziari, culturali, opinioni personali, consumi, predilezioni intellettuali o ludiche, immagini, stati di salute, inclinazioni sessuali, credo religioso, militanze o affinità politiche, stili di alimentazione o d'abbigliamento, attitudini sportive, gusti artistici, letterari o musicali, desideri reali o probabili di un singolo individuo equivale a disporre di un patrimonio cognitivo, dunque di un potenziale mercato di riferimento (ovvero, occorrendo, di un *information asset* di ricatto a tempo debito se il soggetto è interessante), indubbiamente ed enormemente superiore a quello acquisibile dal possesso di solo una o più delle singole tipologie informative sopra sommariamente enunciate. Equivale ad avere in mano la vita intera di un essere umano, la sua intimità, il suo privato esistere, i suoi chiaroscuri di pensiero e di comportamento, i suoi sogni e bisogni insoddisfatti, i suoi desideri inespressi: molto più di ciò che serve per sedurre o intimidire una persona. I Big Data sono e restano comunque dati, la cui origine è tuttavia talora impercettibile al titolare. Si distingue al riguardo fra dati generati dall'interessato (*human generated*), generati dalle macchine (*machine generated*), generati dal meccano economico (*business generated*). I primi sono quelli che scientemente (o scioccamente) gli individui mettono a disposizione nei e dei social network, blog, *multimedia sharing*, siti cc.dd. di recensione (forme di pubblicità non di rado occulta

[23] "Se si vuole modificare il comportamento in Rete delle persone, basta semplicemente alterare sullo schermo gli algoritmi che lo governano, che di fatto regolano il comportamento collettivo o spingono le persone in una direzione preferenziale" (K. Kelly, *L'inevitabile, le tendenze tecnologiche che rivoluzioneranno il nostro futuro*, Milano, 2017, p. 94).

o ingannevole altamente tollerate), portali di *e-commerce*; i secondi sono dati generati dai sistemi di rilevamento (GPS, strumenti scientifici, sistemi di negoziazione borsistica in *high frequency trading*, dispositivi biomedici); i terzi sono infine dati, generati umanamente o meccanicamente, che afferiscono prevalentemente al comportamento economico (pagamenti, ordini, fatturazioni, acquisti e produzioni, vendite, dati bancari e finanziari). Inutile soffermarsi sul potenziale, *in primis* economico, che il possesso di simili profilazioni può arrecare a chi se ne accaparri.

Ma i Big Data non sono i soli a far da mattatori sul palco del web 4.0. L'altro invadente comprimario è l'*Internet of Things*, cioè un insieme di tecnologie che consente, appunto, di far dialogare fra loro le "cose" al fine di consentire agli utenti un loro utilizzo sempre più efficiente, organizzato e funzionale. Il pensiero corre agli assistenti personali intelligenti, ossia ai servizi offerti, ad esempio, da Android (*Google Assistant),* da Apple (*Siri*), da Amazon (*Alexa*), capaci di interpretare il linguaggio naturale e di dialogare con interlocutori umani, allo scopo di fornire informazioni o compiere determinate operazioni. L'assistente personale intelligente (quanto veramente intelligente, poi, è tutto da vedere) è oggi in grado di rispondere alle domande sul meteo o sulle ultime notizie, di ricercare e riprodurre un brano musicale richiesto, di controllare l'impianto di riscaldamento e di condizionamento collegato, di accendere o spegnere le luci o di comandare il ricevitore televisivo dell'utente (c.d. domotica).

Se, allo stato, tali servizi possono anche apparire non così irrinunciabili o coinvolgenti (ma è una valutazione personale, visto il successo commerciale di tale tecnologia), non v'è dubbio che, in un prossimo futuro, con il loro perfezionamento e la loro evoluzione, diverrà pressoché impossibile rinunciarvi (come oggi nessuno, escluse le persone che vivono ai margini delle società, può permettersi di non avere in tasca uno smartphone).

L'aspetto più inquietante è che, mentre i Big Data accumulano e incrociano dati spesso non deliberatamente ceduti dall'interessato, *l'Internet of Things* spinge e spingerà sempre più le persone ad utilizzare nella vita di ogni giorno la rete incrementando la già iperprolifica immissione di nuove informazioni, anche le più intime. Il transito è ben più delicato perché, con l'*Internet of Things* più ancora che con i Big Data, si realizzerà il pieno collegamento fra gli atti quotidiani degli utenti e la loro rivelazione in rete, eventualità che, almeno sino ad oggi, data la necessità di utilizzare sempre un'interfaccia materiale (una tastiera, un telefono, un *tablet*), era senz'altro meno scontata.

In questo mutevole contesto il tema della protezione dei dati personali assume una rilevanza primaria, posto che diventa il presidio irrinunciabile di tutte le libertà classiche e fondamentali contemplate quantomeno dalle

Costituzioni di tutti gli Stati europei. E a questo riguardo, giova dirlo senza remore, la normativa non sa né dare risposte convincenti, né porre argini adeguati. Ecco perché.

6. Dal Codice al GDPR: il rafforzamento dei presidi e la strutturazione dei controlli. Il "baco" dell'interesse legittimo

Nel maggio 2018 qualcosa è accaduto: è divenuto applicabile ai trattamenti eseguiti da tutti gli operatori stabiliti nell'Unione europea il Regolamento 2016/679 UE (GDPR)[24] che, innovando le linee guida della Direttiva 95/46, compie un nuovo salto di qualità. Che una revisione delle regole fosse necessaria era nei fatti. Che tale revisione risulti sufficiente allo scopo è tutto da verificare.

Non è infatti azzardato affermare che la portata protettiva del GDPR sia stata fortemente sopravvalutata.

Gli istituti cardine dei presidi di protezione non risultano strutturalmente variati rispetto alla disciplina pregressa. Risulta invece modificato l'approccio organizzativo imposto agli operatori. Da un lato, essi sono esentati da qualsivoglia obbligo di notifica preventiva e possono beneficiare di una maggiore libertà organizzativa interna; dall'altro, tuttavia, nell'applicazione di una disciplina maggiormente dettagliata anche rispetto ai differenti tipi di trattamento eseguibili sui dati, debbono dotarsi di un più elevato grado di qualificazione professionale anche al fine della vigilanza sui processi. Il tutto condito da una potenziale capacità di controllo e sanzionatoria del Garante ben più accentuata che in passato.

Il trattamento dei dati, oggi come allora, si fonda sul consenso informato e specifico dell'interessato e dunque sul rilascio della preventiva informativa da parte di chi opera il trattamento[25]. Tuttavia i presupposti che in precedenza agivano come sostitutivi del consenso (adempimento di obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati) oggi costituiscono – come noteremo fra un istante – autonome ragioni di liceità del trattamento e appaiono di ampiezza maggiore

[24] In particolare, il Reg. (CE) 27 aprile 2016, n. 2016/679/UE (Regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE), in G.U.U.E. 4 maggio 2016, n. L 119.

[25] Cfr. artt. 6, co. 1°, lett. a), 7, 13 e 14 del Regolamento.

rispetto alle precedenti casistiche di deroga del consenso. Ne consegue che l'informativa agli interessati potrà essere più agile e le richieste di consenso esplicito potranno essere limitate a casistiche più ridotte. A breve il tormentone del consenso si dissolverà come un uragano morente. In una sorta d'infiacchimento progressivo, la legge si adegua alla realtà tecnologica e, non riuscendo a contrastarla né volendo supinamente arrendervisi, può solo tentare di contenerla – anche se talora, come vedremo (par. 8), è costretta ad assecondarla.

Certo, viene confermato il diritto dell'interessato all'accesso ai dati e alla loro rettifica e/o cancellazione[26] e lo si arricchisce con tre ulteriori prerogative. La prima è l'attribuzione del diritto all'oblio (limitato da esigenze connesse alla libertà di informazione, all'adempimento di un obbligo di legge, a motivi di interesse pubblico, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica, ovvero alla necessità della loro conservazione per l'esercizio di un diritto in sede giudiziaria[27]: e dall'ampiezza della deroga già s'intuisce che sparire o farsi dimenticare sarà un'eventualità piuttosto remota). La seconda prerogativa è il diritto alla limitazione del trattamento (ove esso non sia necessario per l'esecuzione del contratto) e, insieme e all'opposto, il diritto di portabilità dei dati (che dovrebbe consentire agli interessati, ad esempio, di trasferire assai agilmente ad altro provider di servizi *in cloud* i dati personali in precedenza affidati ad un concorrente)[28]. La terza prerogativa aggiunta è un particolare diritto di opposizione al marketing diretto ovvero al trattamento finalizzato alla profilazione, anche automatizzata, dell'interessato. Allo stesso modo l'opposizione è possibile rispetto a processi automatizzati che abbiano ad oggetto l'assunzione di decisioni inerenti le persone fisiche[29].

Accanto alle tradizionali figure del titolare e del responsabile del trattamento[30], s'affianca oggi il responsabile della protezione dei dati (il *Data*

[26] Cfr. artt. 12 e 16 del Regolamento.

[27] Cfr. art. 17 del Regolamento.

[28] Cfr. artt. 18 e 20 del Regolamento

[29] Cfr. artt. 21 e 22 del Regolamento. Tali previsioni sono fortemente innovative rispetto alla previgente disciplina in quanto hanno ad oggetto non già le finalità del trattamento dichiarato dal titolare ovvero la natura dei dati personali trattati, bensì – appunto – le modalità di trattamento automatizzato finalizzato alla profilazione del cliente ovvero all'assunzione di decisioni che ineriscono il cliente. L'oggetto di tutela, in questo caso, è la possibilità di opporsi ad un trattamento automatizzato che possa generare un nuovo dato riferito all'interessato (profilazione) o che possa determinare scelte del titolare funzionali, ad esempio, all'instaurazione di un rapporto giuridico con l'interessato (ad esempio, la concessione di un finanziamento). Processo che, per effetto dell'opposizione dell'interessato, non può essere affidato ad analisi automatizzate ma deve richiedere l'intervento ponderato e di merito "umano".

[30] Cfr. artt. 24, 26 e 28. In questo contesto si segnala l'intervenuta esplicitazione normativa

Protecion Officer, DPO), soggetto contraddistinto da "conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati", indipendente rispetto all'operatore, che svolge una funzione di controllo rispetto ai processi, consulenziale a favore delle funzioni interne dell'operatore e di relazione rispetto all'Autorità Garante[31].

La maggiore e forse unica, vera novità riguarda l'imposta organizzazione degli operatori che, nei processi interni e con modalità documentate, dovrebbero a loro volta imporre il *privacy check* in ordine a qualsivoglia iniziativa da intraprendere e sviluppare per valutarne gli impatti di trattamenti dei dati e i connessi rischi, individuando eventuali presidi che si rendessero necessari (la chiamano *privacy by design*). Siffatta impostazione organizzativa aziendale dovrebbe essere quella maggiormente garantista, volta cioè a raccogliere e trattare esclusivamente i dati personali degli interessati che siano strettamente necessari (*privacy by default*), prevedendo, ove possibile e compatibilmente con gli scopi, processi di pseudonimizzazione, di cifratura o di anonimizzazione dei dati personali (complice strizzatina d'occhio ai Big Data), in coerenza con il principio di minimizzazione dei trattamenti[32]. In tale contesto, quindi, la raccolta di dati personali qualificati come "facoltativi" (prassi oggi ancora largamente applicata nei formulari di molte aziende) sarebbe contraria al principio sopra espresso risultando infatti incompatibile con l'obiettivo di minimizzazione dei trattamenti (primo fra tutti la stessa raccolta). Permangono ovviamente gli obblighi di adozione di misure di sicurezza proporzionate al rischio, da stimarsi ora attraverso una documentabile valutazione d'impatto, che non esige però la previa notifica al Garante. Da ultimo, in conformità alla fonte disciplinare (cioè un regolamento europeo), che in ragione della sua diretta applicabilità consente (dovrebbe consentire) piena uniformità tra le discipline nazionali dei vari Stati, viene ammessa, e anzi favorita, una organizzazione infragruppo delle procedure privacy interne, che rende lecita la comunicazione alle differenti società di uno stesso gruppo dei dati personali della clientela, laddove ciò sia giustificato da funzionalità operative egualmente suddivise fra le varie società del gruppo e ciò corrisponda al principio di minimizzazione dei trattamenti dei dati personali. Non è un caso, del resto, che la disciplina preveda espressamente la condivisione infragruppo di un medesimo DPO, con il solo limite della sua capacità di eseguire materialmente, su ogni stabilimento, le veri-

riferita al verificarsi di contitolarità del trattamento, fattispecie in precedenza comunque riconosciuta in forza della "giurisprudenza" del Garante Privacy.

[31] Cfr. artt. 37 e ss. del Regolamento.

[32] Cfr. artt. 25 e 32 del Regolamento.

fiche e i controlli di rito e di svolgere regolarmente l'attività consultiva che il medesimo è tenuto a rendere alle diverse funzioni aziendali.
Se le novità non appaiono sconcertanti, sconcerta invece il sottile ed esiziale *pied de porc* con cui di fatto si scardinano molti gangli del sistema. Alludiamo al concetto, *rectius*: all'esimente del cosiddetto "interesse legittimo" del titolare dei dati rispetto a trattamenti anche non esplicitamente consentiti dall'interessato[33].
Se è vero che il GDPR prevede che il legittimo interesse del titolare possa costituire il fondamento di un trattamento dei dati purché sia assicurato il bilanciamento fra diritti del titolare e diritti dell'interessato, non è men vero che il precedente assetto normativo (art. 24, lettera g) Codice Privacy) richiedeva che i trattamenti senza consenso avvenissero solo nei casi precisamente individuati dalle norme. Il GDPR consegna invece alla bilancia dei titolari del trattamento questo gravoso compito di ponderazione senza però escludere un postumo intervento sanzionatorio o correttivo del Garante stesso. In base al Considerando 47 del GDPR, infatti, il trattamento basato su legittimi interessi dispensa dal consenso dell'interessato alla duplice condizione che: (1) non siano in gioco interessi, diritti o libertà fondamentali dell'interessato (tenuto conto delle ragionevoli aspettative dello stesso in ragione della sua relazione col titolare del trattamento); (2) e l'interessato sia informato della possibilità di tale trattamento senza però una specifica rivelazione dei metodi con cui verrà tarata la bilancia di stima.
Il riferimento al "legittimo interesse" amplia, quindi, in termini assai significativi la possibilità di dar corso ad un trattamento senza preventivo consenso dell'interessato atteso che, in via esemplificativa, lo stesso Considerando 47 precisa che "può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto", fattispecie, nella vigenza dell'anteriore Codice Privacy, viceversa impraticabile in assenza di consenso esplicito.
La svolta, qui, è veramente radicale, anzi: più che una svolta è un'autentica inversione di tendenza e di filosofia regolamentare. Il consenso, pur nelle sue devianti percezioni applicative, rappresenta il suggello decisivo della

[33] Cfr. art. 6 del Regolamento che individua le basi giuridiche, tra cui il consenso dell'interessato, in presenza delle quali il trattamento dei dati personali può dirsi lecito. Tra le basi giuridiche menzionate, particolare rilevanza merita il richiamo al "legittimo interesse del titolare del trattamento o di terzi" che autorizza il trattamento dei dati degli interessati "a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore". Tale previsione assume la rilevanza di una "norma di chiusura" che sostanzialmente rende non tassativo l'elenco dei presupposti menzionati dall'art. 6.

proprietà del dato. L'introduzione di una così ampia nozione di interesse legittimo comporta un eguale e contrario affievolimento della centralità del consenso, dunque una implicita ma chiara svalutazione progressiva della natura proprietaria del dato. E non è tutto, perché nel suddetto apprezzamento dei contrapposti interessi il titolare del trattamento è solo, nel senso che non sussistono parametri certi di riferimento[34]. La sua responsabilizzazione corrisponde appieno alla deresponsabilizzazione del Garante, ma non anche alla preclusione della postuma facoltà di quest'ultimo di sindacare la scelta del titolare. Ne consegue lo scivolamento su un terreno giuridicamente magmatico, dove se non sarà agevole per il titolare difendersi da una contestazione di abuso di legittimo interesse, neppure l'interessato o il Garante avranno gioco facile nel dimostrare l'opposto. Né basta a restituire ordine e misura al meccano bilancistico il diritto dell'interessato, sancito dal Considerando 70, di opporsi, sempre e senza costi, al trattamento dei suoi dati personali né l'inversione dell'onere probatorio (spetta al titolare del trattamento dimostrare che i suoi interessi legittimi prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato). E per quanto alcune linee guida siano desumibili da precedenti provvedimenti del Garante[35], resta l'amaro retrogusto di una scelta salomonica e ambigua, che non troppo difficilmente potrebbe ricondursi ad un forzato obiettivo di liberalizzazione proprio di quei fenomeni particolarmente invasivi ed espropriantì come i Big Data o l'*Internet of Things*. Come dire: non possiamo impedirli, se non a patto di precludere l'inarrestabile avanzata dei colossi IT, neppure possiamo cedere, se non a patto di perder la faccia come legislatori o regolatori, *ergo* elargiamo un *laissez-faire* circondato da qualche ridondante ma vago limite e, se proprio qualcuno esagererà, potremo sempre intervenire a bocce ferme.

A questo apparato, molto imbarazzato e lievemente ipocrita, il legislatore italiano ha cercato di porre un rattoppo. Con la legge di bilancio 2018[36], sono stati previsti a carico e a beneficio di chi tratti dati personali mediante mezzi automatizzati o nuove tecnologie sulla base dei legittimi interessi, rispettivamente l'obbligo di una preventiva notifica al Garante corredata di

[34] Flebile al riguardo appare il riferimento, contenuto nel cit. Considerando 47, all'esistenza di "una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento".

[35] Così, ad esempio, Provv. in materia di videosorveglianza 8.4.2010 (G.U n. 99 del 29 aprile 2010) e Provv. generale prescrittivo in tema di biometria 12.11.2014 (G.U. n. 280 del 2 dicembre 2014).

[36] Art. 1 commi da 1020 a 1024 L. 27 dicembre 2017, n. 205 (G.U. n. 302 29.12. 2017 – S.O. n. 62).

una nota informativa conforme a modelli e linee guida che il Garante avrebbe dovuto predisporre e una sorta di silenzio assenso tale per cui, decorsi 15 giorni dalla notifica, il trattamento avrebbe potuto comunque aver luogo (salve ovviamente le postume verifiche del Garante). Paradossalmente, per rammendare una norma vaga e corriva, si ritorna al burocratico e imbelle modello della notifica.
Da qui un ulteriore passo indietro: il D.Lgs. 10 agosto 2018, n. 101, che allineerà il Codice Privacy al GDPR, disporrà che, dal 25 maggio 2018, le norme di cui ai commi 1022 e 1023 dell'art. 1, L. cit., si applichino esclusivamente ai trattamenti dei dati personali funzionali all'autorizzazione del cambiamento del nome o del cognome dei minorenni, nei limiti e con le modalità di cui all'articolo 36 del GDPR (consultazione preventiva del Garante), con buona pace dei modelli e delle linee guida che il Garante avrebbe dovuto pubblicare e che in realtà non lo furono affatto. Dunque un ulteriore restringimento dello spettro di protezione poco prima, sia pur debolmente, ampliato.
Il risultato netto di questo andirivieni normativo è uno solo: la solenne affermazione di proprietà del dato personale non corrisponde più, né nei fatti né nelle regole, ad una reale attribuzione dominicale. Il perimetro di tutela del dato, già di per sé non esteso (cfr. par.1), subisce un'ulteriore e significativa contrazione.

7. La tutela "privatistica" dell'apparato normativo sulla protezione dei dati personali nella realtà liquida di Internet

Prescindendo da questa stortura in odore di *deregulation* forzata, le disposizioni poc'anzi analizzate rispecchiano e rispettano il principio finalistico enunciato in chiusura al par.1, per il quale la disciplina sulla tutela dei dati personali è volta, non già, a creare privacy ma a contribuirvi, evitando che terzi non autorizzati entrino in possesso di quei dati che i titolari legittimi siano autorizzati a trattare. Si tratta della canalizzazione della circolazione dei dati personali più ampiamente illustrata in esordio.
Non v'è dubbio che il GDPR integri, sulla carta e sempre con salvezza di quel lasco lasciapassare, uno strumento normativo più efficiente ed efficace di attuazione della suddetta protezione: vuoi in quanto in grado di uniformare le discipline dei singoli Stati aderenti all'UE, vuoi in quanto – in concreto – a partire dal principio di minimizzazione, volto a conferire agli interessati strumenti più efficaci per controllare, limitare, inibire la circolazione dei dati personali, alcuni loro trattamenti e ad imporre agli

operatori un livello di controllo qualificato e sanzioni potenzialmente rilevanti in caso di omissione.
Sarebbe però assai miope e ingenuo ritenere che la soluzione sia stata raggiunta o che l'apparato in essere consenta e garantisca la voluta contribuzione ai riconosciuti diritti alla riservatezza. Il varco aperto dalla nuova esimente dell'interesse legittimo dà una chiara misura di quanto il GDPR sia stato sopravvalutato. Vi sono poi fattori circostanti che lasciano fortemente dubitare dell'efficienza del nuovo impianto regolamentare.
In primo luogo, si tratta pur sempre di una normativa che si rivolge essenzialmente al ristretto vecchio continente e che, per converso, ha ad oggetto una realtà di reti di comunicazione assai "liquide" ove il rischio di trasferimenti illegittimi, perdite o di trafugamenti di dati è sempre in agguato. In secondo luogo, per la natura del bene protetto, una volta perduto il canale di circolazione autorizzato (la strada lecita), il ripristino non è più possibile. Pur con tutti i presidi oggi possibili e immaginabili la sicurezza di una rete di dati che dialoga con un server non può ritenersi assimilabile alla sicurezza che può essere garantita ad un bene fisico che si voglia preservare. Si pensi, più semplicemente, al caso di trafugamento, o di comunicazione a terzi non autorizzata, dei codici di accesso (username e password) di titolarità degli interessati: in questo caso, non c'è alcuna possibilità di soluzione al ripristino della riservatezza se non quella di procedere alla modifica, da parte degli utenti, di tali codici per prevenire il ripetersi del fenomeno, ma una volta che i dati personali da proteggersi siano stati, per qualsivoglia ragione, rivelati a terzi, la privacy è definitivamente perduta.
A parte questa forse scontata, ma a nostro avviso ineluttabile e significativa, considerazione, deve poi valutarsi il fatto che, come già per la L. 675/1996 e il Codice, la disciplina del GDPR è, nei termini descritti, riservata ai soggetti privati che operano i trattamenti di dati. L'art. 23 del GDPR, infatti, consente ai singoli Stati di imporre limitazioni agli specifici principi e diritti di informazione e di accesso riservati agli interessati, ove ciò sia necessario e proporzionato in una società democratica, per la salvaguardia della sicurezza pubblica, per le attività di prevenzione, di indagine e di perseguimento di reati o per l'esecuzione di sanzioni penali. Le deroghe sono ammesse in caso di violazioni della deontologia professionale e per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno stato membro, di un interesse economico o finanziario rilevante, per la tenuta di registri pubblici, per ragioni di interesse pubblico generali. In considerazione del richiamo operato dall'art. 23 anche all'art. 5 del GDPR, la deroga può spingersi sino a comprendere, in tutto o in parte, i principi generali riferibili al trattamento di dati personali ivi indicati e, quindi, può pervenire a disegnare,

in tali ipotesi, specifiche aree in cui i diritti degli interessati, di fatto, non sono, o sono solo parzialmente, esercitabili.
Il tenore delle norme sospinge ad una duplice considerazione: da un lato, la disciplina sulla protezione dei dati personali, che pure ebbe il merito di riconoscere agli stessi un preciso valore proprietario salvo oggi ridurne la portata, non è idonea, quantomeno per l'impossibilità di garantire il pieno controllo del web e di coloro che vi operano, a rendere la rete un luogo sicuro e, tantomeno, a proteggere gli utenti da utilizzi illegittimi e dalle conseguenze dannose derivanti da tali utilizzi. Dall'altro lato, e in ogni caso, i vincoli, gli obblighi e i limiti di utilizzo dei dati personali di terzi, per effetto della deroga di cui all'art. 23 del GDPR, sono riferiti esclusivamente ai soggetti privati che operano al di fuori di quelle finalità ivi descritte e per le quali la deroga è ammessa. E poiché fra le finalità contemplate ricadono, oltre (più che giustamente) a quelle riferite alla commissione di reati e alla sicurezza pubblica, anche (più opinabilmente) quelle di interesse economico o finanziario rilevante e più in generale, di interesse pubblico, il potenziale ambito derogativo risulta, di fatto, marcatamente ampio e imprevedibilmente ampliabile.
In questo contesto, pur semplificando il rilievo, si può tratteggiare la contrapposizione fra una tutela superiore riferita agli interessati nei confronti dei soggetti privati e, viceversa, una – a nostro avviso inaccettabile – tutela minorata riferita agli interessati nei confronti dei soggetti pubblici o, meglio, anche di quei soggetti non pubblici ma che, nella lata accezione del GDPR, operino o possano operare nell' "interesse pubblico". Questa primazia dell'interesse pubblico, allargato e allargabile, rispetto ai diritti fondamentali degli interessati protetti dalla disciplina lascia quantomeno perplessi, se non inquieti. Essa si colloca comunque nell'alveo di quella progressiva svalutazione della proprietà del dato cui s'informa il nuovo impianto regolamentare. E un esempio illuminante e fresco di debutto sta nell'obbligo di fatturazione elettronica: strumento che non garantirà un vero contrasto dell'evasione e che anzi stimolerà sciaguratamente il ricorso al sommerso, che già molto è costato ai contribuenti onesti, ma che offrirà allo Stato un tremendo arnese di tracciamento accentrato della vita dei singoli. E il debole parere del Garante[37], nello stabilire che il fisco non potrà a suo piacimento controllare i dati, ha tutta l'aria di una tremula foglia di fico, spazzabile via da un delicato, segreto e semplice click.

[37] Provv. del 20 dicembre 2018 denominato "Provvedimento in tema di fatturazione elettronica" e reperibile sul sito web del Garante Privacy.

8. L'inesorabile processo di spossessamento del dato fra libero arbitrio, pseudo-volontà, costrizioni tecniche e impotenze o compiacenze normative. Il fenomeno della "dispersione concentrativa"

Giunto a questo punto, il lettore ha ogni più sacrosanto diritto di porre una domanda e pretendere una risposta. La domanda è: perché mai, a fronte di questi possenti strumentari legali, perché mai la privacy non c'è? Perché siamo, sempre e ovunque, controllati e controllabili, tracciati e tracciabili? Perché la legge "non ci protegge"?

La risposta è complessa e semplice al tempo stesso e ci riconduce al punto di partenza: la proprietà del dato.

Accanto all'imponente impianto normativo per come evolutosi nel tempo, e anzi, quasi paradossalmente, in costante parallelo a tale evoluzione, lo "spossessamento" progressivo dei dati personali è inesorabilmente cresciuto. Se la norma afferma solennemente la proprietà del dato (salvo ora indebolirla grazie all'ambiguo lasciapassare dell'interesse legittimo: *supra* par. 6), la tecnologia, con sottili blandizie, spinge sempre di più gli individui a cederlo. E ove le blandizie non bastino, è la stessa legge che, piegandosi all'avanzata tecnologica, forza o asseconda questo processo di cessione.

Il fenomeno ha radici risalenti che muovono dall'esplosione dei *reality show*, mirabilmente stigmatizzata nella paradigmatica pellicola di Peter Weir. Attraverso l'illusione della notorietà (il famoso "quarto d'ora di celebrità" teorizzato da Andy Warhol e/o Nat Finkelstein), l'individuo viene portato a cedere alla telecamera – non nascosta come nel caso del Signor Truman bensì presente, visibile e "voluta" dal protagonista – pressoché tutta la sua intimità: il nome è l'ultimo e forse il meno importante dei dati a fronte di una sceneggiatura improvvisata e basata propriamente sull'ostensione di ogni attitudine, ideologia, atteggiamento, costume di vita, segreto, in pratica di ogni dato personale che l'individuo di norma tiene gelosamente per sé.

Siffatto processo di "spossessamento indotto" passa attraverso due raffinate chiavi di persuasione psicologica. Per un verso, si trasmette il convincimento che non aver altro merito che cedere i propri dati non soltanto può essere lucroso (concorrenti e/o vincitori di solito vengono profumatamente pagati) ma è addirittura un gioco: tanto è normale essere "spiati" (leggasi: farsi volutamente spiare) che la cessione dei dati diventa un fenomeno ludico. Per altro verso si crea un'assuefazione collettiva e contagiante (all'esibizionismo del partecipante fa da insostituibile contraltare il voyeurismo dello spettatore) che sempre più normalizza il processo di "libera" cessione del dato. E nelle ultime versioni di questa neoforma di spettacolo, la norma-

lizzazione è accresciuta, secondo un curioso meccano di ribaltamento del concetto stesso di notorietà, proprio dalla presenza di personaggi già noti ma che vengono spinti essi stessi a rivelare lati e aspetti di vita, cioè nuovamente dati e informazioni, che esulano dalla cessione dei dati connessa alla loro attività professionale o artistica, quest'ultima, ma solo quest'ultima, necessariamente pubblica.

Se il *reality show* crea l'habitat di germinazione, saranno e sono invece le reti sociali ad espandere il fenomeno su scala planetaria. La tecnica di induzione alla cessione è ancor più sottile e legalmente più invasiva, specie nell'ambito delle reti cc.dd. generiche. A fronte della possibilità di soddisfare bisogni latamente narcisistici, le reti non soltanto consentono la pubblicazione e la divulgazione (talora con conseguenze drammatiche per gli interessati) di articoli, immagini, commenti, opinioni ma acquisiscono anche una "licenza" sui materiali pubblicati. Siamo di fronte ad un fenomeno di *trade-off* quasi invisibile (l'invisibilità sta nel fatto che la cessione del dato è inserita in condizioni generali di contratto che quasi nessun utente legge limitandosi alla spunta della casella di consenso per subito accedere, famelico, al suo coriandolo di *Lebensraum* virtuale) ma fortemente invasivo e abilmente catturante: l'utente crede di poter esprimere se stesso a costo zero, mentre il costo è rappresentato esattamente dalla cessione dei propri dati.

L'induzione alla cessione si tramuta spesso in forzatura implicita. L'esempio più eclatante è dato da quelle applicazioni il cui utilizzo è subordinato alla messa a disposizione del gestore dei contatti dell'utente conservati nel dispositivo portatile di quest'ultimo. Senza tale cessione l'applicazione diventa, a seconda dei casi, inaccessibile, inutilizzabile o non più utilizzabile. Tale fenomeno – considerato quasi normale per effetto del procedimento d'assuefazione dianzi evocato – solleva un problema di non poco momento. Se A possiede nella sua rubrica telefonica nomi, immagini, indirizzi e numeri di B, C e D, nel momento in cui A cede quei dati al gestore dell'applicazione in realtà non cede dati propri bensì dati di terzi senza che B, C e D abbiano necessariamente espresso il loro consenso alla disponibilità di una cessione al di fuori dell'utilizzazione dei loro dati da parte, e solo da parte, di A verso gli stessi B, C e D. L'impianto normativo tradisce qui un limite apparentemente logico ma dagli effetti dirompenti: la disciplina privacy, si è detto, non trova infatti applicazione fra persone fisiche, tuttavia l'uso che il singolo utente potrebbe fare dei dati di altri porta ad una involontaria e praticamente infinita possibilità di viralizzazione indesiderata[38].

In tutte le casistiche sin qui esaminate – e con salvezza del tema appena

[38] Sempre fatta salva l'ignorata e irrisolta, e che tale resterà, contraddizione evocata nella nt. 11.

richiamato – lo spossessamento del dato si realizza pur sempre su base volontaristica: la legge non può intervenire giacché, una volta affermato il principio della proprietà del dato, non è possibile limitarne la disponibilità da parte del legittimo proprietario.

Ma esistono tecnologie di impiego quotidiano dove la libera formazione del consenso è fortemente affievolita dall'architettura stessa del veicolo tecnologico. L'ausilio di un navigatore o di un sistema antifurto satellitare comporta necessariamente il trasferimento dei dati di spostamento, l'uso di un telefono cellulare (sia o meno attivato il segnale di geolocalizzazione) realizza lo stesso effetto, il pagamento effettuato con una carta di credito rende tracciabili i consumi di un individuo, il pedaggio autostradale pagato con mezzi elettronici, egualmente e sia pur con minor invasività, permette di ricostruire il movimento della persona. In questi casi si assiste ancora ad una cessione formalmente volontaria ma nei fatti forzosa se non a patto di porre l'individuo nella condizione di non poter interagire coi mezzi, gli unici mezzi, ormai accreditati dall'impiego sociale: dunque una volontà coatta o, se si preferisce, una coazione volontaristica che tuttavia, sul piano squisitamente legale, non trova un limite perché non è appunto possibile negare che la cessione sia comunque la conseguenza di una scelta del proprietario del dato.

Non c'è scampo neanche per i più eroici riottosi che, quando vogliono consultare qualunque sito internet (il che ormai è divenuto imprescindibile anche solo per bisogni professionali), si trovano costretti ad accettare i famigerati cookie, micro-file che leggono le navigazioni ritrasferendo i dati al server di partenza e la cui accettazione si rende spesso indispensabile per poter agevolmente o interamente consultare il sito. Il Garante[39] non ha potuto fare altro che imporre un obbligo di trasparenza, in termini di precisa informativa all'utente circa l'uso dei cookie e i loro effetti, ma la regolamentazione qui cede il passo all'imperativo tecnologico e non può arrischiarsi a vietare l'impiego di un mezzo tecnico sul quale si basa la (illusoria) gratuità della rete. È pur vero che il cookie non recepisce i dati di una specifica persona ma di una macchina (uno stesso computer può, e anzi normalmente è, utilizzato da più persone all'interno di un nucleo familiare o di un piccolo contesto aziendale), ma è altrettanto vero che esso concorre alla formazione di quel patrimonio conoscitivo disperso e concentrato (diverrà chiaro fra breve il senso di questa apparente aporia) su cui si fondano i nuovi modelli di sviluppo economico e di controllo sociale.

[39] Provv. 8.5.2014 "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie", in vigore dal 2 giugno 2015.

Quando non interviene o non forza, la legge spesso si fa complice del processo di spossessamento, offrendo nuove opportunità (nella specie blandizie legislative) che si ritrasformano in trappole per gli utenti. Un recente esempio nasce dal D.Lgs. 15 dicembre 2017, n. 218 attuativo della Direttiva 2015/2366/UE meglio nota come seconda *Payment Service Directive*, in breve PSD2)[40].
La norma ha introdotto nuove figure di intermediari che s'interpongono nei servizi di pagamento per semplificare l'operazione o per offrire al cliente una panoramica della propria situazione finanziaria. Nel primo caso, si tratta di un *Payment Initiator Service Provider* (PISP), al quale l'utente cede le sue credenziali di accesso a un conto in modo tale che, ogni volta che intenderà effettuare un pagamento on line, si risparmierà il fastidio di digitare numeri e codici di una carta di credito prepagata, dovendo semplicemente premere un tasto che gli permetterà di eseguire il pagamento istantaneo tramite il PISP. Nel secondo caso, l'*Account Information Services Provider* (AISP) riceve dall'utente i dati di accesso a tutti i conti che quest'ultimo detenga presso diversi intermediari: ciò permetterà all'utente, con un solo click, di avere un'immediata e completa visione delle sue disponibilità liquide senza l'incomodo di dover accedere a ciascun sito dei depositari e usare una calcolatrice per fare le somme. Servizi utili e spicci, che ovviano alle piccole seccature, ma che aumentano i rischi e accentuano quella che chiameremo, con un ossimoro apparentemente inestricabile, *dispersione concentrativa*.
I rischi aumentano, intuitivamente, perché il trasferimento di credenziali a terzi (rigorosamente vietato dalla precedente Direttiva PSD1) innesta un canale di comunicazione ulteriore rispetto a quello fra banca e cliente, dunque raddoppia le opportunità di *hackering*.
La dispersione concentrativa merita invece una riflessione più ampia.
Gli esempi testé addotti non sono che una sfaccettatura, importante ma non unica, della tendenza fattuale e della compiacenza normativa rispetto non solo all'appropriazione del dato ma anche alla sua concentrazione: in altre parole, i nostri dati sono sempre più *concentrati* e quindi immediatamente aggregabili a fini profilativi (spesso con automatismi che generano risultati devianti) ma, al tempo stesso, sono sempre più *dispersi* perché sempre più disponibili, in forme e quantità sempre più aggregate presso più soggetti, dunque più "noti" oltre che più aggredibili e comunque più sfruttabili dai detentori. La dispersione concentrativa è la semente dei Big Data e il concime dell'*Internet of Things*. Se i primi nascono dalla combinazione interferenziale di dati diversi per tipologia e scaturigine, ogni seduzione, induzione o

[40] Relativa ai servizi di pagamento nel mercato interno e che abroga la precedente Direttiva 2007/64/CE (PSD) (G.U.U.E. 23 dicembre 2015).

costrizione, prodotta dal secondo, alla cessione dei dati nei confronti di uno stesso soggetto facilitano le interferenze e le profilazioni ma nel contempo aumentano anche il livello di tracciabilità degli interessati e in egual misura diminuiscono il loro patrimonio di riservatezza. Anche l'emittente di una carta di credito conosce entità, frequenza, tipologia e quantità dei nostri acquisti, ma se a questo peculio conoscitivo si aggiungesse quello relativo alle spese compiute con altre carte di credito oppure agli estratti conto bancari, il suo potere di condizionamento nei nostri confronti aumenterebbe a dismisura. Come il rischio di investimento finanziario si riduce attraverso la diversificazione degli impieghi, parimenti la protezione dei dati aumenta quanto più frammentata ne sia la disponibilità da parte dei terzi. Se investissimo tutti nostri risparmi in un solo titolo anche molto redditizio, potremmo godere di una lucrosa rendita ma se quel titolo, per qualsivoglia ragione, crollasse, l'intero nostro patrimonio finanziario s'azzererebbe. Analogamente, accettando o dovendo accettare una sempre più pronunciata dispersione concentrativa dei nostri dati, il nostro tesoro di riservatezza svanisce, la sua ricchezza si trasferisce a pochi altri, la nostra ostentata bandiera di libertà va in brandelli. La risposta alla legittima domanda del lettore diviene perciò semplice e semplicemente disarmante. La legge non protegge realmente i nostri dati semplicemente perché ce ne ha resi padroni, ma la nostra signoria su di essi, per incoscienza, vanagloria, costrizione tecno-sociale o deliberata riduzione regolamentare (v. interesse legittimo), nei fatti svanisce: siamo noi, assai volenti o *obtorto collo*, a volere o dovere rendercene cedenti.

9. Bilancio di un ventennio: è mai stata o sarà mai vera privacy?

Le (a torto chiamate) distopie letterarie o cinematografiche non dovrebbero essere solo un *divertissement* evasivo o uno scacciapensieri accreditato dalla *fictio*. Dovrebbero invece farci riflettere.
In un mondo non lontano, anzi quanto mai prossimo, smetteremo di andare al cinema perché i network a pagamento ci spediranno pellicole usa e getta via *cloud*, non frequenteremo più negozi perché l'e-commerce li soppianterà[41],

[41] Amazon ha da poco inaugurato un nuovo metodo di vendita: si possono ordinare più capi di abbigliamento, provarseli e poi restituire quelli non graditi. Quando compriamo musica on line, possiamo concederci il lusso di dimenticarci brani simili che ci piacerebbero: è il computer a suggerirceli dopo ogni acquisto. In Cina si sta avviando la massiccia sperimentazione di *little brother devices*, che vantano la capacità di decrittare i gusti del cliente a partire dagli atteggiamenti del volto che guarda un prodotto (sia pur secondo una scala di misurazione del tutto arbitraria e incapace di cogliere le infinite sfumature dell'emozione umana): v. M. Sideri, *La*

i ristoranti si ridurranno a laboratori culinari perché neoschiavi in risciò ci serviranno a domicilio, viaggi e mostre diventeranno obsoleti grazie alla realtà virtuale o aumentata, persino il sesso potrà praticarsi a distanza grazie ad apparecchiature che consentiranno di trasmettere e ricevere stimoli fisici per via elettronica. In banca abbiamo già smesso o quasi di andarci da un pezzo. Invitiamo chi reputasse questo dipinto come l'ennesima, divertente distopia a confrontare le sue abitudini di vita di quindici o vent'anni fa con quelle attuali, a rammentare quante volte negli anni più recenti si è recato in edicola per comprare un giornale, quante volte è andato in banca per effettuare un bonifico, quante volte ha guardato il televisore per accertarsi del meteo e quante volte lo ha fatto invece consultando lo smartphone, quante volte si è recato in libreria e quante volte ha ordinato libri on line. Di questo passo la dispersione concentrativa dei dati diverrà più che normale, i big data si costruiranno da soli, la privacy cesserà di esistere, dunque neppure sarà più necessario regolarla[42].

Questa cosmica *partouze* informativa, simile ad una *dark room* dove non è neppure dato scegliere i partner occasionali, dove si coltiva l'illusione di contatti ma prospera il virus dell'isolamento umano (concetto ben diverso dall' "essere lasciati soli"), cesserà prima o poi di eccitare e produrrà una crisi di rigetto. Almeno è ciò che l'umanità deve augurarsi.

I primi segnali di un'inversione di tendenza non mancano, soprattutto fra i *millenials* o le generazioni Z, sempre meno attratte da una virtualità già venuta a noia e sempre più sedotte, più che dai beni, dalle *experiences*, dalle sensazioni fisiche, dirette, emotive. Cresce però anche il numero di utenti della rete che ricorrono ai filtri anti-tracciamento e anti-pubblicitari (le stime viaggiano fra il 40 e il 45% degli internauti). S'innalza il livello di autodifesa: nessun dato è proteggibile neppure coi più sofisticati sistemi, la sola possibilità di ridurre i danni è salvare quotidianamente i propri dati su supporti fisici esterni alla rete. Gli algoritmi si rendono responsabili di scelte abnormi e screditanti[43] e c'è già chi suggerisce di boicottarne gli automatismi immettendo dati, commenti e notizie contraddittorie e

macchina delle emozioni che riconosce che tipo (di cliente) sei, in *Corriere della Sera*, 10.3.2019.

[42] Illuminanti queste sagge parole: "La sorveglianza si trasferisce dall'eccezionale al quotidiano, dalle classi "pericolose" alla generalità delle persone. La folla non è più "solitaria" e anonima: è "nuda". La digitalizzazione delle immagini, le tecniche di riconoscimento facciale consentono di estrarre il singolo dalla massa, di individuarlo e di seguirlo. Il *data mining*, l'incessante ricerca di informazioni sui comportamenti di ciascuno, genera una produzione continua di "profili" individuali, familiari, territoriali, di gruppo. La sorveglianza non conosce confini" (S. Rodotà, *op. cit.*, p. 4).

[43] Cfr. sul tema S. U. Noble, *Algorithms of oppression*, New York University Press, New York, 2018.

spiazzanti per la logica di un sistema impostato su parametri di coerenza elementare[44].

La crescente resistenza privata all'invasività dei sistemi comunicativi è l'unica risposta che la legge, malgrado ogni più meritorio sforzo, non saprà mai né mai potrà dare. Vent'anni di regole minuziose e progressive hanno migliorato soltanto il rapporto di riservatezza fra privati ma non hanno impedito il processo d'appropriazione globale che quelle regole non hanno saputo, ma forse neppure voluto, prevenire. Il vuoto normativo è qui colmato, in parte, solo da questa atipica legittima difesa che non s'avvale di strumenti legali ma di mezzi di reazione tecnologica.

Negli ultimi tempi abbiamo assistito ai pianti di coccodrilli pingui, ex signori della rete che, arricchitisi con essa, non hanno esitato a ripudiarla in nome di una privacy tradita. Si può capirli: una montagna di dollari val bene un *mea culpa*. Fra il 7 e l'8 marzo di quest'anno, un po' dopo il disastro di *Cambridge Analytica*, Zuckerberg ha annunciato un cambio epocale di Facebook: più tutela della privacy, comunicazioni criptate, sicure e protette, anche se nel frattempo il più grande social network mondiale s'appresta a lanciare la sua criptovaluta[45]. Ma è del 9 marzo la notizia più raggelante: la *Data Protection Commission* (DPC), ossia il Garante privacy irlandese, si trova nell'occhio del ciclone (alimentato nientemeno che da Merkel e Vestager) per la corriva vigilanza sui giganti tecnologici che hanno sede nell'isola alla quale apportano, in cambio di tassazioni irrisorie, un'indispensabile fetta di Pil in via diretta e indotta. Chiosa il nostro Garante, Antonello Soro: il GDPR ammette norme nazionali integrative che rischiano di far riemergere la tendenza delle aziende a trarre vantaggio dalle asimmetrie normative[46]. Con buona pace del celebrato Regolamento unionista che avrebbe dovuto eliminare ogni dislivello normativo e scongiurare il *privacy shopping*.

È mai stata o sarà mai vera privacy? L'ardua sentenza non spetterà né ai posteri, né ai legislatori, né ai giudici: apparterrà ai byte, ai server e agli algoritmi o, più verosimilmente e sperabilmente, all'umana intelligenza e all'umano buon senso. Gli unici dati che, oggi, sembrano veramente perduti.

[44] Si veda lo spassoso, ma non troppo, consiglio di depistaggio algoritmico proposto da P. Battista, *Il caso Facebook, l'algoritmo? Possiamo imbrogliarlo*, in *Corrriere della Sera*, 22.3.2018.
[45] M. Gaggi, *Zuckerberg svolta e torna alla privacy*, in *Corriere della Sera*, 8.3.2019.
[46] D. Casati e M. Pennisi, *Al molo dove finisce la privacy*, in *Corriere della Sera*, 9.3.2019.