Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei *social media*, tra regole generali e ricerca di una specificità*

Privacidade e novas tecnologias, uma relação difícil. O caso emblemático das redes sociais, entre as regras gerais e a busca de uma especificidade.

Paolo Passaglia§

1. Considerazioni generali, sul contesto (e sulla delimitazione del tema)

Trattare della *privacy* in rapporto alle nuove tecnologie è esercizio quanto mai arduo. Per molteplici motivi. In primo luogo, si pone una difficoltà quasi di ordine psicologico, legata alla sensazione di un progressivo, ma inesorabile ridimensionamento della sfera entro cui gli strumenti giuridici possono valere a proteggere diritti individuali: non pare improprio, infatti, assumere che l'introduzione di nuove forme di comunicazione costituisca una costante ipoteca sulla inviolabilità della propria sfera privata e – soprattutto – sulla controllabilità della circolazione dei propri dati[1].

---

* Relazione svolta nel corso delle *IX Jornadas italiana-española-brasileña*, dedicate a «*El Derecho a la Intimidad*», svoltesi a Madrid nei giorni 22 e 23 settembre 2016.

§ Professore associato di Diritto pubblico comparato presso l'Università di Pisa.

1 L'evoluzione del concetto di «*privacy*», e segnatamente il passaggio dal *right to be let alone* alla controllabilità del trattamento dei propri dati, è tema troppo ampio per poter essere anche solo sinteticamente analizzato

In secondo luogo, caratteristica connaturata alla ricerca è la sua provvisorietà, legata all'impossibilità di proporre una pur minima ipostatizzazione: se ne ha una dimostrazione patente pensando a quanto il quadro di riferimento tecnologico vada assumendo contorni semplicemente impensabili anche solo pochi anni fa; ma l'evoluzione tecnico-scientifica è, in realtà, solo una componente del dinamismo che anima il contesto, giacché processi sociali affatto diversi incidono in maniera decisiva sulla *privacy*: un riferimento paradigmatico è, in proposito, quello alle esigenze di sicurezza collettiva, che sempre più marcatamente si intrecciano con l'utilizzo delle nuove tecnologie.

Una terza ragione di difficoltà risiede nella proliferazione di frontiere operative su cui la tematica della *privacy* si misura: la crescente pervasività delle tecnologie, ed in specie delle tecnologie della comunicazione, all'interno della società contemporanea moltiplica inevitabilmente le sedi nelle quali la *privacy* viene in gioco, sedi che sovente richiedono di impostare il bilanciamento con contrapposte esigenze in termini differenziati. A complicare ulteriormente la ricerca si pone l'onere per lo studioso di verificare se e quanto il progresso tecnologico e le nuove forme di comunicazione richiedano effettivamente l'elaborazione di regole nuove ovvero se le nuove esigenze possano essere decrittate alla luce di regole e principi già enucleati in relazione ad ambiti più tradizionali nei quali la *privacy* viene in gioco: per fare solo uno dei molteplici esempi che potrebbero prospettarsi, si pensi al contemperamento tra *privacy* ed attività giornalistica, per il quale un compiuto schema giuridico è venuto costruendosi nel corso degli anni, ma che non sembra pianamente applicabile in via estensiva al *web-journalism*[2].

Sullo sfondo di queste problematiche si stagliano, tuttavia, questioni che trascendono la *privacy*, ma che sulla *privacy* hanno un impatto troppo marcato per essere taciute. Problematiche che attengono, in generale, all'inquadramento giuridico delle nuove tecnologie, a proposito delle quali è con sempre maggiore affanno che gli strumenti regolativi tradizionalmente propri delle liberal-democrazie riescono a rispondere agli *inputs* sociali. Su questo punto specifico, poi, la panoramica inerente alle nuove tecnologie mostra assetti normativi sempre più frastagliati, sia per l'aumento dei livelli di governo chiamati ad intervenire (si pensi all'influenza della normativa sovranazionale, in particolare di matrice euro-unitaria, sui regimi nazionali) sia, soprattutto, per la disseminazione di centri produttivi di norme, centri dai quali promanano regole che si ha sovente non poche riserve finanche a qualificare come riconducibili al fenomeno giuridico (al punto di premettere l'aggettivo «*soft*» proprio per rimarcare le peculiarità di questo «*law*», ferma restando l'opportunità non di rado riscontrabile di esprimersi nei più vaghi termini di «modelli di comportamento»). E, come in un sistema perfettamente osmotico, ciò che vale per le nuove tecnologie si ripropone, in termini sostanzialmente identici, anche per la *privacy*, quanto meno (sebbene non solo) nella misura in cui la relativa disciplina si associ alle nuove tecnologie.

Tanto dirompenti sono le questioni connesse a questi ultimi rilievi che il parlare oggi di *privacy* e nuove tecnologie suggerisce di prestare attenzione, in primo e decisivo luogo, a come si compone il mosaico normativo (e para-normativo) destinato a sorreggere le soluzioni da apportare di volta in volta, in relazione a tale o a talaltra frontiera operativa. Questa, almeno, è la sensazione di chi scrive; una sensazione che si riverbera sulle scelte che hanno improntato il presente lavoro: senza che possa darsi un inventario di ragioni che fondino scientificamente le scelte operate, il riferimento a quanto si è venuti dicendo permette di cercare di tratteggiare qualche giustificazione, atta – lo si auspica – a dar conto della non arbitrarietà dell'approccio che si è inteso seguire.

---

in queste pagine. Ci si limiterà, quindi, a darlo per presupposto, rinviando a molti degli altri contributi che sono presentati nel presente incontro.

2 Sul tema, per una analisi insieme teorica e casistica, v., in part., M. PAISSAN (a cura di), *Privacy e giornalismo. Libertà di informazione e dignità della persona*, 3ª ed., Roma, ed. Garante per la protezione dei dati personali, 2012.

Due sono, in particolare, le giustificazioni che si avvertono come più solide.

Innanzi tutto, il prospettare un'analisi anche blandamente organica dell'intreccio tra tutela della *privacy* ed uso delle nuove tecnologie sarebbe un obiettivo davvero troppo ambizioso, almeno per le competenze di chi dovrebbe qui perseguirlo, giacché la multiformità degli ambiti interessati sarebbe tale da richiedere un esame grandangolare della disciplina della *privacy*, presumibilmente da estendere, almeno in fase di premessa, anche agli ambiti più tradizionali, dai quali i principi e le regole potrebbero e/o dovrebbero in parte dedursi. Con il che, peraltro, si andrebbe pure a produrre una inopportuna sovrapposizione con gli altri contributi programmati.

Inoltre, la compenetrazione sempre più inestricabile tra diritto nazionale (ai vari livelli) e diritto sovranazionale ingenera il rischio che una analisi organica basata sui contenuti concreti della disciplina risulti, in buona misura, sovrapponibile con quella che potrebbe essere proposta dal versante spagnolo, il che forse potrebbe essere riguardato alla stregua di una inutile iterazione.

In definitiva, l'approccio che pare più proficuo è quello di verificare, non già il risultato – in termini di disciplina concreta – del mosaico di norme e modelli di comportamento, bensì la trama del mosaico che si compone in relazione alle singole tematiche in cui la *privacy* viene in gioco nel quadro delle nuove tecnologie. E, nello spirito di un intervento evocativo, più che descrittivo, ad essere trattate saranno alcune fattispecie, che, al di là del loro interesse intrinseco (non maggiore, probabilmente, di quello di alcune tematiche oggetto di pretermissione), si appalesano significative, vuoi per la loro peculiarità vuoi per la loro esemplarità. Il tutto privilegiando aprioristicamente le tecnologie che possono dirsi più «nuove», con conseguente sacrificio per altre, magari ancora di maggiore impatto sociale (solo per citare un esempio emblematico, le intercettazioni telefoniche), che vengono più facilmente associate a fenomeni ormai consolidati.

Nella – probabilmente vana – ricerca di un filo conduttore che offra alla trattazione un grado minimo di unitarietà, si è ritenuto di poter filtrare le considerazioni che verranno proposte attraverso la lente dei *social media*, che presentano il duplice vantaggio di aprire una serie di problematiche che possono dirsi comuni all'intera rete e, al contempo, di stimolare l'enucleazione di talune particolarità rispetto al più generale diritto dell'*Internet*[3-4].

2. (Segue:) un sistema di protezione fluido

La scelta qui operata di concentrarsi sul sistema regolativo delle forme (e dei limiti) entro cui si prospetta la tutela della *privacy* in connessione con l'utilizzo delle nuove tecnologie (e con i *social media* in ispecie) non può non partire dalla constatazione della grande fluidità del sistema, percorso da una serie composita di tendenze, tra le quali, in particolare, spiccano: il moto ascendente – verso l'Unione europea – della regolamentazione, soprattutto per ciò che attiene alla individuazione dei

3 Per una ricostruzione della nascita e dell'evoluzione dei *social media*, v. M. MASSAROTTO, *Social Network*, Milano, Apogeo, 2011; G. RIVA, *I social network*, Bologna, il Mulino, 2ª ed., 2016.

4 L'impatto dei *social media* sul diritto è oggetto di sempre maggiore attenzione da parte della dottrina giuridica, generalmente oscillante tra una riconduzione della tematica al diritto generale della rete, da un lato, e la formulazione di una serie di precisazioni e l'individuazione di una serie di specificità, dall'altro. Oltre ai contributi focalizzati su aspetti determinati, possono segnalarsi lavori rivolti ad una analisi del fenomeno a più ampio spettro: cfr. R. CAFARI PANICO ET AL., *Da Internet ai Social Network. Il diritto di ricevere e comunicare informazioni e idee*, Rimini, Maggioli, 2013; S. LANDINI – M. MARRAFINO, *Social Media e Diritto*, *ebook*, Altalex, 2015; per una sintesi, v. A.R. POPOLI, *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. informazione e informatica*, 2014, 981 ss.

principi conformativi della materia; una certa «fuga» dal formante legislativo[5], corollario della difficoltà per quest'ultimo di rispondere efficacemente alle costantemente rinnovate sfide poste dalla tecnologia; la crescita numerica, ma soprattutto di importanza dei provvedimenti generali e para-giurisdizionali di organi deputati ad assicurare il rispetto della *privacy* nella concreta dinamica dei rapporti sociali, organi che, nell'ordinamento italiano, trovano la propria massima espressione nell'Autorità Garante per la protezione dei dati personali.

Dalle tematiche che possono evocarsi, e che di seguito verranno in parte prese in esame, emerge il coesistere di queste tendenze ed il loro diverso calibrarsi di volta in volta. Ne discende un quadro assai poco sistematico, fatto di soluzioni divergenti in punto di logica del sistema delle fonti: a fronte di questa disorganicità, resta da valutare il grado di efficacia che questo mosaico riesce a spiegare in concreto per la protezione della *privacy*. Anche in proposito, il caso dei *social media* offrirà spunti che non appaiono privi di interesse.

Prima di soffermarsi sull'ambito prescelto, qualche ulteriore considerazione si impone, però, sul panorama normativo che va delineandosi concretamente. Da esso si prenderanno le mosse, anche per l'individuazione delle problematiche, all'interno dei *social media*, su cui converrà appuntare precipuamente l'attenzione.

3. Il nuovo regolamento euro-unitario

Per parlare di *privacy* e di nuove tecnologie è forse opportuno partire dalla fine. Anzi, dal futuro prossimo, e cioè dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, «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 (regolamento generale sulla protezione dei dati)», entrato in vigore nel maggio di quest'anno, ma applicabile – ai termini del suo art. 99, comma 2 – a partire dal 25 maggio 2018.

L'adozione di questo regolamento[6] segna una tappa quanto mai significativa, sia per la forma che per il contesto. La forma, innanzi tutto: il passaggio prodottosi da una direttiva ad un regolamento indica chiaramente l'avvertita esigenza di predisporre un quadro normativo il più possibile uniforme in tutta l'Unione, a testimonianza della ormai matura consapevolezza della insufficienza di un inquadramento che sia essenzialmente nazionale della protezione della *privacy*. Proprio al riguardo emerge l'importanza del contesto, che il progresso tecnologico ha semplicemente *rivoluzionato* rispetto a quello nel quale la direttiva del 1995[7] si muoveva, ma anche rispetto a quello che era stato tenuto presente al momento dell'adozione delle direttive 2002/21/CE[8] e 2002/58/CE[9], e successive modifiche, le quali, con la direttiva del 1995, hanno formato per molto (troppo?) tempo il tessuto connettivo della protezione dei

5 Il riferimento va, ovviamente, alla teoria dei formanti elaborata da Rodolfo Sacco, su cui v., ora, R. SACCO, *Legal Formants: A Dynamic Approach to Comparative Law*, in *American Journal of Comparative Law*, 1991, n. 1, 1 ss., e n. 2, 343 ss.

6 Sul quale, v., per un primo commento, M. IASELLI, *Privacy: cosa cambia con il nuovo regolamento europeo*, *ebook*, Altalex, 2016.

7 Direttiva 95/46/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

8 Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro).

9 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 (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

dati personali con riguardo alle comunicazioni elettroniche. Il recentissimo regolamento vuole essere la risposta normativa, organica e – per quanto possibile – compiuta, a quella massa di *inputs* sociali moltiplicatisi ed articolatisi in ragione dello sviluppo delle potenzialità della *Information and communications technology*.

Come è chiaro, il regolamento è destinato ad avere un impatto notevole sulla concreta disciplina del trattamento dei dati personali. Sarebbe difficile, del resto, non riconoscere la portata delle novità introdotte. In questa sede, tuttavia, più che soffermarsi su singoli profili dell'impianto normativo del regolamento, si ritiene che possa essere utile rimarcare il significato di questo atto, il quale, se è vero che risponde all'esigenza di strutturare uno *jus commune* europeo, è anche vero che non segna un cambiamento radicale per ciò che attiene al *quantum* di autenticamente normativo si trova nei modelli di comportamento che conformano la prassi del trattamento dei dati personali.

Proprio quest'ultimo aspetto merita di essere evidenziato, nella misura in cui è indice di una tendenza che appare ormai ineluttabile al progressivo abbandono dei paradigmi normativi tradizionali in favore di modelli di comportamento che sono annoverabili, al più, nello schema del *soft law*. In tal senso, non può non rilevarsi l'elevato numero di rinvii che il regolamento reca a codici di condotta, il che non suona certo come una novità, né in riferimento ai pregressi interventi delle istituzioni euro-unitarie né avendo riguardo alla disciplina interna[10]. Ma non si tratta di una semplice conferma: il *quid pluris* rispetto a questi precedenti è costituito dal fatto che il regolamento è stato concepito proprio in chiave di normativizzazione di un contesto in cui si avvertivano lacune regolative; da ciò si deduce che, se questa normativizzazione a livello europeo non ha prodotto una significativa contrazione degli spazi per l'autodisciplina, l'immagine che viene alla mente è quella di un gioco a somma zero tra livelli di regolamentazione (nel senso che l'attrazione a livello sovranazionale del «giuridicamente disciplinabile» produce, in definitiva, quasi solo l'effetto di essiccare i margini di manovra dei poteri normativi nazionali), assortita dalla sanzione della (definitiva?) abdicazione dell'*hard law* in relazione ad una serie di ambiti connessi alla *privacy* nello spettro delle nuove tecnologie.

I modi e l'entità di una tale abdicazione variano, ovviamente, a seconda delle tematiche specifiche che si affrontino. Anche solo scorrendo il regolamento, in effetti, emerge come l'impatto della normativa approntata presenti un grado sensibile di mutevolezza, oscillando dalla ricerca di una quasi-codificazione[11] all'abbandono espresso, passando per un silenzio che lascia, sì, impregiudicata la possibilità di un intervento conformativo, ma che, allo stato, finisce per produrre i risultati di una acquiescenza nei confronti di una regolamentazione proveniente da fonti diverse. Con riferimento ai *social media*, le velleità di codificazione non sono evidentemente state sollecitate; l'articolazione e la complessità del tema rendono, comunque, impossibile ricondurre ad unità l'impostazione adottata: complessivamente, pare di poter dire che il regolamento, pur non restando del tutto inerte, non è riuscito

10 Con riguardo a «la "giuridicizzazione" delle regole deontologiche nella legislazione», in particolare ad opera del Codice della *privacy*, v., di recente, A. BELLELLI, *Il problema della giuridicità delle regole deontologiche delle professioni*, in M. NUZZO (a cura di), *Il principio di sussidiarietà nel diritto privato*, vol. I, Torino, Giappichelli, 2014, spec. 84 ss.

11 Un esempio tra i più indicativi di questa dimensione è dato dalla ricerca di una regolamentazione del diritto all'oblio, espressamente contemplato dall'art. 17 del regolamento euro-unitario, il cui tessuto normativo evidenzia lo sforzo di fornire un quadro giuridico sufficientemente preciso da indirizzare una prassi, che si è finora orientata sulla base di quanto la Corte di giustizia ha avuto modo di affermare, segnatamente nella sentenza *Google Spain*, causa C-131/12, del 13 maggio 2014, come attuata attraverso le *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia EspaÑola de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, adottate, il 26 novembre 2014, dal Gruppo di lavoro *ex* Articolo 29, e come concretizzata a livello nazionale (in special modo da parte dell'Autorità Garante, stante la pressoché totale assenza di decisioni rese di recente da parte di giudici italiani).

a penetrare in maniera compiuta nella materia, lasciando così sussistere, in larga misura, vecchie incertezze.

4. Regolamento euro-unitario e *social media*: un rapporto complesso

Se è fin troppo scontato affermare che uno dei canali principali nei quali si estrinseca l'utilizzo delle nuove tecnologie è quello dei *social media*, già questo rilievo pare sufficiente per dar conto dell'importanza di un sistema di tutela della *privacy* che coinvolga anche questi strumenti. Non può dunque non sorprendere che il regolamento euro-unitario, non solo non affronti espressamente la questione, ma anzi tenda ad escluderla dal suo ambito di applicazione. Il *considerando* 18, testualmente ripreso poi dall'art. 2, par. 2, lett. *c*), è, al riguardo, quanto mai esplicito: «il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale». Nel medesimo *considerando* si precisa ulteriormente che «le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei *social network* e attività *online* intraprese nel quadro di tali attività».

Si fa salva comunque l'applicazione del regolamento «ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico».

La normativa che ne risulta è, per quanto attiene all'ambito di applicazione, sostanzialmente coincidente con gli approdi cui è giunta la prassi nella vigenza della direttiva del 1995. Si ha, in sostanza, un forte elemento di continuità, a proposito del quale non è ozioso interrogarsi in termini di effettiva opportunità rispetto alle problematiche che sono emerse e, soprattutto, che potrebbero venire in essere in futuro. Sul piano teorico, pare difficile contestare che si sia persa un'occasione importante: la rivisitazione *ab imis* della normativa euro-unitaria sulla *privacy* si prestava senz'altro a diventare un momento atto a chiarire i contorni dell'applicabilità della stessa ad un settore, quale quello dei *social media*, già molto sviluppato, ma soprattutto in grande espansione. Sul piano concreto, poi, la mancata definizione dell'ambito di applicabilità lascia aperti interrogativi non trascurabili sulla protezione della *privacy* in relazione alle attività poste in essere sui *social*, in special modo per quanto concerne la disciplina da applicare effettivamente alle singole attività, imponendosi sovente una scelta, quasi *caso per caso*, legata all'individuazione delle attività che possono farsi rientrare tra gli oggetti disciplinati dal regolamento, di quelle che, pur nella loro peculiarità, possono conoscere una sorta di applicazione analogica, anche *pro parte*, del regolamento e di quelle per le quali, invece, la disciplina è da individuarsi al di fuori, sovente per il tramite di una tendenziale equiparazione tra attività poste in essere nel mondo virtuale e corrispondenti attività del mondo reale.

4.1. L'ambito di applicazione: la conferma delle vecchie incertezze

Onde chiarire l'impatto che il regolamento ha sui *social media*, è da rimarcare, innanzi tutto, la pressoché completa sovrapponibilità con la direttiva del 1995 delle definizioni di alcuni concetti-chiave. Il riferimento va, in primo luogo, al «trattamento» dei dati personali[12], ma alle medesime conclusioni

12 Le differenze tra il testo dell'art. 4, n. 2), del regolamento e l'art. 2, lett. *b*), della direttiva sono, almeno ai presenti fini, assolutamente di dettaglio, come si evince dalle indicazioni che si riportano in corsivo all'interno del testo attualmente vigente: «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi

deve giungersi con riguardo alla nozione di «titolare del trattamento», in tutto equivalente al precedente «responsabile del trattamento»[13], ed a quella di «responsabile del trattamento», corrispondente al precedente «incaricato del trattamento»[14].

Se a questa congruenza si aggiunge quella inerente alla sopra accennata *household exemption*[15], il quadro che emerge è quello di una conferma del regime precedente, e dunque un implicito avallo di quelle letture dell'ambito di applicazione che erano state fatte in riferimento ai *social media*. Tra tutte, la più chiara era anche quella probabilmente più autorevole, per quanto priva di carattere autoritativo, tratteggiata nel parere 5/2009 – WP 163 «sui *social network on-line*», adottato il 12 giugno 2009 dal Gruppo di lavoro per la tutela dei dati *ex* art. 29[16].

Nel documento si sono individuate tre categorie di «responsabili» (nella terminologia più recente, «titolari») del trattamento. La prima corrisponde ai fornitori di *social network services*, i quali, per un verso, «mettono a disposizione i mezzi per l'elaborazione dei dati degli utenti e forniscono tutti i servizi di base relativi alla gestione degli utenti (per esempio, la registrazione e la cancellazione degli account)», e per l'altro «determinano […] il modo in cui i dati degli utenti possono essere usati a fini pubblicitari e commerciali» (ivi inclusa la pubblicità fornita da terzi)[17]. La seconda categoria comprende i fornitori di applicazioni «che funzionano in aggiunta a quelle degli SNS e se gli utenti decidono di servirsene»[18].

Tanto la prima quanto la seconda categoria possono dirsi delimitate in misura soddisfacente, in ragione della loro individuazione mediante criteri essenzialmente formali, ma – soprattutto – *ex ante* identificabili. Il discorso si complica non poco con la terza categoria. Recita il parere: «la direttiva [oggi: il regolamento] non estende gli obblighi del responsabile [oggi: del titolare] del trattamento a chi elabora dati personali "per l'esercizio di attività a carattere esclusivamente personale o domestico" – la cosiddetta "esenzione domestica"»; ciò posto come regola generale, tuttavia, si aggiunge che, «in alcuni casi, è possibile che queste attività non siano più coperte dall'esenzione e si può allora ritenere che

---

automatizzati e applicate a dati personali *o insiemi di dati personali* [aggiunto], come la raccolta, la registrazione, l'organizzazione, *la strutturazione* [aggiunto], la conservazione, *l'adattamento* [in precedenza: "l'elaborazione"] o la modifica, l'estrazione, la consultazione, *l'uso* [in precedenza: "l'impiego"], la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, *la limitazione* [in precedenza: "il congelamento"], la cancellazione o la distruzione».

13 V. il raffronto (nei modi di cui alla nota precedente) tra l'art. 4, n. 7), del regolamento e l'art. 2, lett. *d*), della direttiva: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, *singolarmente* [in precedenza: "da solo"] o insieme ad altri, determina le finalità e *i mezzi* [in precedenza: "gli strumenti"] del trattamento di dati personali*;* [in precedenza la cesura tra i periodi consistenza in un punto] quando le finalità e i mezzi di *tale* [in precedenza: "del"] trattamento sono determinati *dal diritto dell'Unione o degli Stati membri* [in precedenza: "da disposizioni legislative o regolamentari nazionali o comunitarie"], il *titolare* [in precedenza: "responsabile"] del trattamento o i criteri specifici applicabili *alla* [in precedenza: "per la"] sua designazione possono essere *stabiliti dal diritto dell'Unione o degli Stati membri* [in precedenza: "fissati dal diritto nazionale o comunitario"]».

14 È quanto emerge dal confronto, nelle forme già sperimentate alle note che precedono, tra l'art. 4, n. 8), del regolamento e l'art. 2, lett. *e*), della direttiva: «la persona fisica o giuridica, l'autorità pubblica, il servizio o [eliminato: "qualsiasi"] altro organismo che *tratta* [in precedenza: "elabora"] dati personali per conto del *titolare* [in precedenza: "responsabile"] del trattamento».

15 La lettera del precitato art. 2, par. 2, lett. *c*), del regolamento è identica alla previsione che figurava all'art. 3, par. 2, della direttiva.

16 Il testo del parere, in italiano, è consultabile *on line* alla pagina *www.privacy.it/grupripareri200905.html* (tutti i riferimenti ai *links* presenti nello scritto sono aggiornati all'ultimo accesso del 31 luglio 2016).

17 Cfr. parere 5/2009 – WP 163 «sui *social network on-line*», cit., par. 3.1.

18 *Ibidem*.

all'utente dell'SNS incombano alcuni obblighi del responsabile [*id est*, del titolare] del trattamento»[19].

L'apertura ad eccezioni rispetto alla regola implica, ovviamente, possibili incertezze, cui lo stesso parere ha cercato di far fronte riportando «qualche esempio», a titolo, presumibilmente, soltanto indicativo, lungi dunque da ogni pretesa di esaustività.

Il primo esempio è quello dell'utilizzo del *social network* «come piattaforma di collaborazione per un'associazione o una società»: la limitazione dell'esenzione domestica alle sole persone fisiche rende qui incontestabile la sussistenza di una eccezione alla regola[20]. Come incontestabile, almeno in linea di principio, è anche l'esempio successivo, inerente all'uso del servizio di *social network* «soprattutto come piattaforma a fini commerciali, politici o filantropici»[21]: la distanza rispetto all'utilizzo «domestico», chiara in teoria, non è detto però che lo sia in concreto, ben potendo certe espressioni «personali» confondersi con attività di uno dei tipi citati. L'incertezza si accresce ulteriormente, e non di poco, con il terzo esempio, relativo al caso in cui «l'accesso ai dati (profilo, messaggi, contenuti, ecc.) inseriti da un utente», anziché essere «limitato ai contatti che l'utente stesso ha scelto», è esteso in ragione del fatto che «l'utente può acquisire molti contatti di soggetti terzi, alcuni dei quali del tutto sconosciuti»: infatti, «un numero elevato di contatti può indicare che l'esenzione domestica non si applica e che l'utente va quindi considerato un responsabile [leggasi, ora, titolare] del trattamento»[22]. Per grandi linee, il concetto sembra chiaro: se sono molti i soggetti che possono accedere a determinati dati, chi li mette a disposizione non può trincerarsi dietro il carattere «personale o domestico» della sua attività; resta però del tutto impregiudicata una concretizzazione di quei «molti contatti» che fanno scattare l'applicazione della normativa sul trattamento dei dati. Il rischio di affidare la quantificazione a valutazioni eminentemente soggettive di funzionari amministrativi e/o di organi giurisdizionali è tutt'altro che trascurabile: a seconda del tipo di dati e della persona coinvolta, la definizione dei «molti» può integrarsi anche con un numero non particolarmente elevato di contatti; a rendere la concretizzazione particolarmente insidiosa è, però, soprattutto l'impossibilità di misurare i contatti di «secondo grado», nel senso che nulla esclude che un numero limitato di contatti possa rivelarsi comunque un veicolo di diffusione estremamente efficace, allorché uno dei pochi contatti abbia, a sua volta, un gran numero di collegamenti all'interno del *network*, con il che un dato «domestico» per chi lo immette diviene un dato «di dominio pubblico» per chi si limita all'attività di condivisione.

Né viene in soccorso l'ulteriore esempio menzionato, relativo a «quando l'accesso alle informazioni del profilo non si limita ai contatti scelti, come nel caso in cui tutti gli iscritti all'SNS hanno la possibilità di consultare un profilo o i relativi dati possono essere indicizzati da motori di ricerca»[23]: la fattispecie, in realtà, reca due realtà molto diverse, l'una ancorata ad una scelta (il carattere pubblico dell'*account*) riconducibile all'utente, anche se talora indotta da impostazioni di *default* del *service provider*, mentre l'altra del tutto estranea all'utente, in quanto collegata alla struttura del *social network* ed all'interazione da esso stabilita con uno o più motori di ricerca.

In definitiva, ciò che emerge è l'esistenza di un buon numero di zone grigie sulle quali un intervento normativo avrebbe potuto (e probabilmente dovuto) far chiarezza, e non solo nell'ottica di una precisa determinazione delle eccezioni alla *household exemption*, ma anche in riferimento ai contenuti stessi di quest'ultima, la quale, nel disegnare uno spazio di *libertà* (?!) per gli utenti che si avvalgano dei servizi offerti a titolo personale e domestico, non può escludere che fenomeni di triangolazione in sé non illeciti

19 *Ibidem*.
20 *Ivi*, par. 3.1.1.
21 *Ibidem*.
22 *Ibidem*.
23 *Ivi*, par. 3.1.2.

portino a trattare dati sotto la copertura della *household exemption* che finiscono per entrare a far parte del bagaglio informativo di chi poi li disseminerà. Per tacere, tra l'altro, di chi, grazie alla condivisione, sarà nelle condizioni di usarli addirittura per fini commerciali.

Che si tratti di un'occasione persa appare, in definitiva, quanto mai evidente; alcune delle conseguenze di questa omissione potranno forse essere colte anche già nei paragrafi che seguono. In essi, l'analisi dovrà essere condotta costantemente confrontandosi con un'obiezione di fondo, implicita ma ben presente, e soprattutto di forte impatto, in tutta la sua semplicità: se l'attività dei *providers* e quella di matrice commerciale degli utenti sono oggetto di disciplina, attraverso l'applicazione della normativa posta dal regolamento euro-unitario, una regolamentazione specificamente rivolta ai *social networks* è davvero necessaria?

La domanda è certamente insidiosa, potendo far leva sul fatto che un intervento specifico, per un verso, rischierebbe di produrre una inutile duplicazione di norme, se riferito – anche solo in parte – ai soggetti già interessati, e, per altro verso, se si andasse invece a regolamentare l'attività degli utenti «ordinari», il pericolo di comprimere la libertà individuale oltre il lecito non potrebbe essere escluso *a priori*. Nell'affrontare le problematiche che si evocheranno, questa riserva dovrà essere costantemente tenuta in considerazione.

4.2. L'estensione ai *social media* delle norme generali sul diritto della rete: la specificità trascurata

Circoscritto, nelle forme che si sono viste, l'ambito di applicazione ai *social media* del regolamento euro-unitario, il passo successivo per delineare il mosaico normativo pare che debba essere quello di spiegare l'assenza di una disciplina specificamente dedicata ai *social*. E, nella ricerca di una coerenza dell'impianto complessivo, l'ipotesi da formulare è quella della sua inutilità: sul presupposto della inopportunità di infrangere la *household exemption*, l'essenziale della regolamentazione delle attività in essi compiuta, anche in relazione alla tutela della *privacy*, dovrebbe poter essere rintracciato nel tessuto normativo generale, dettato tanto dal regolamento quanto da altre fonti, e segnatamente da quelle richiamate dallo stesso regolamento[24]. Una tale impostazione è lungi dal potersi dire originale, giacché è andata fortemente caratterizzando la prassi, come dimostra, tra gli altri, lo stesso parere 5/2009 – WP 163 «sui *social network on-line*» del Gruppo di lavoro per la tutela dei dati *ex* art. 29[25].

Ora, l'estensione ai *social media* della normativa generale può apparire, per così dire, «rassicurante», nella misura in cui permette agli operatori di orientare le proprie condotte su schemi già consolidati. Il punto è che, per un verso, gli schemi non sempre appaiono così consolidati e, per l'altro, l'idea di trattare i *social media* come il resto della rete assume talvolta (ed in specie proprio per quel che concerne il trattamento dei dati) i contorni di una forzatura.

Per cercare di illustrare le riserve appena espresse, conviene prospettare un confronto tra due decisioni, rese a poche settimane di distanza, relativamente a due fattispecie assai diverse, ma con taluni non secondari punti di intersezione: la sentenza della Corte di giustizia sul caso *Google Spain*[26] e la

24 Solo per fare un esempio – peraltro non dei più anodini – potrebbe venire in soccorso una citazione dell'art. 2, par. 4: «Il presente regolamento non pregiudica […] l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva».

25 Cfr., in particolare, il par. 5, espressamente dedicato all'«Applicabilità delle direttive CE».

26 Grande Sezione, sentenza 13 maggio 2014, *Google Spain SL e Google Inc. c/ Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12. La sentenza ha da subito catalizzato l'attenzione della dottrina europea. Tra i moltissimi contributi della dottrina italiana, da segnalare è, in particolare, G.

sentenza della Corte di cassazione italiana sul caso *Vivi Down c. Google*[27].

Il profilo che qui interessa consiste, segnatamente, nella determinazione dei confini del concetto di trattamento dei dati e nell'individuazione del responsabile (ora, del titolare).

La Corte di giustizia era chiamata, nel quadro di una questione pregiudiziale di interpretazione, a valutare se il motore di ricerca fosse o meno tenuto ad eliminare, dai risultati delle ricerche recanti nella *query* il nome di una persona, risultati concernenti vicende ormai remote.

Nel rendere la propria decisione, la Corte di giustizia ha rilevato che «il gestore di un motore di ricerca "raccoglie" dati [personali], che egli "estrae", "registra" e "organizza" successivamente nell'ambito dei suoi programmi di indicizzazione, "conserva" nei suoi *server* e, eventualmente, "comunica" e "mette a disposizione" dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche»: «tali operazioni […] devono essere qualificate come "trattamento" […], senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali»[28]. Nessuna rilevanza, in proposito, è stata riconosciuta al fatto «che tali dati abbiano già costituito l'oggetto di una pubblicazione su *Internet* e non vengano modificati dal suddetto motore di ricerca»[29]; e poiché «è il gestore del motore di ricerca a determinare le finalità e gli strumenti […] del trattamento di dati personali che egli stesso effettua […], […] è di conseguenza lui a dover essere considerato come il "responsabile" [leggasi, ora, "titolare"] di tale trattamento»[30].

D'altra parte – ha proseguito la Corte – «è pacifico che tale attività dei motori di ricerca svolge un ruolo decisivo nella diffusione globale dei dati […], in quanto rende accessibili questi ultimi a qualsiasi utente di Internet che effettui una ricerca a partire dal nome della persona interessata, anche a quegli utenti che non avrebbero altrimenti trovato la pagina *web* su cui questi stessi dati sono pubblicati»[31].

In definitiva, «nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti *web*, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni [in tema di trattamento dei dati], affinché le garanzie previste […] possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata»[32].

Qualche settimana prima, la Corte di cassazione italiana aveva avuto modo di interrogarsi su problematiche affini. Il caso verteva sul video postato da un utente su *Google Video*, avente ad oggetto uno studente diversamente abile, deriso dai compagni di classe, i quali rivolgevano considerazioni infamanti anche all'associazione Vivi Down, associazione che ha come oggetto sociale precipuo quello della tutela dei diritti delle persone affette dalla sindrome di Down. Il video era stato rimosso dopo circa

---

RESTA – V. ZENO ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, RomaTrE-Press, 2015.

27 Sezione III penale, sentenza 17 dicembre 2013 – 3 febbraio 2014, n. 5107, consultabile *on line* sul sito *Diritto penale contemporaneo*, alla pagina *www.penalecontemporaneo.it/upload/1392109339vividown_Redacted_st.pdf*, con il commento di A. INGRASSIA, *La sentenza della Cassazione sul caso Google* (6 febbraio 2014), *www.penalecontemporaneo.it/area/3-/19-/-/2817-la_sentenza_della_cassazione_sul_caso_google/*.

28 Grande Sezione, sentenza 13 maggio 2014, causa C-131/12, cit., par. 28.

29 *Ivi*, par. 29.

30 *Ivi*, par. 33.

31 *Ivi*, par. 36.

32 *Ivi*, par. 38.

due mesi, durante i quali era però rimasto a disposizione del pubblico. Uno dei procedimenti giudiziari innescati dalla vicenda riguardava i dirigenti della divisione italiana di Google, accusati di aver leso la reputazione del protagonista del video e dell'associazione e di non aver adempiuto agli obblighi imposti dalla normativa sul trattamento dei dati.

In primo grado, i dirigenti erano stati condannati dal Tribunale di Milano[33], sull'assunto che l'indicizzazione dei risultati delle ricerche facesse ricondurre a Google l'identificazione del responsabile (ora: titolare) del trattamento dei dati personali dello studente diversamente abile. La condanna era stata annullata dalla Corte d'appello di Milano[34], contro la cui decisione era stato proposto ricorso per cassazione[35].

La Corte di cassazione, attraverso un coordinamento tra la normativa europea (e la relativa normativa nazionale di attuazione) in tema di *privacy*[36] ed in tema di commercio elettronico[37], ha confermato la sentenza della Corte d'appello.

Ad avviso della Suprema Corte, «se non vi è dubbio che il concetto di "trattamento" sia assai ampio, perché comprensivo di ogni operazione che abbia ad oggetto dati personali, indipendentemente dai mezzi e dalle tecniche utilizzati, il concetto di "titolare" è, invece, assai più specifico, perché si incentra sull'esistenza di un potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati»: «titolare del trattamento non è chiunque materialmente svolga il trattamento stesso, ma solo il soggetto che possa determinarne gli scopi, i modi, i mezzi»[38].

Degli obblighi connessi al trattamento dei dati «è destinatario in modo specifico il solo titolare del trattamento e non ogni altro soggetto che si trovi ad avere a che fare con i dati oggetto di trattamento senza essere dotato dei relativi poteri decisionali»[39].

Ciò vale anche per «la figura dell'*Internet hosting provider*, perché esso è definito […] come colui che si limita a prestare un "servizio consistente nella memorizzazione di informazioni fornite da un destinatario del servizio"». Ad avviso della Corte, «il gestore del servizio di *hosting* non ha alcun controllo sui dati memorizzati, né contribuisce in alcun modo alla loro scelta, alla loro ricerca o alla formazione del file che li contiene, essendo tali dati interamente ascrivibili all'utente destinatario del servizio che li carica sulla piattaforma messa a sua disposizione»[40].

La Cassazione ha quindi desunto, «ai fini della ricostruzione interpretativa della figura del titolare del trattamento dei dati, che il legislatore ha inteso far coincidere il potere decisionale sul trattamento con la capacità di concretamente incidere su tali dati, che non può prescindere dalla conoscenza dei dati stessi», con il che, «finché il dato illecito è sconosciuto al *service provider*, questo non può essere

33 Sezione IV penale, sentenza 24 febbraio – 12 aprile 2010, imp. Drummond et al. La sentenza è consultabile *on line* alla pagina *www.giurcost.org/casi_scelti/Google.pdf*.

34 Sezione I penale, sentenza 21 dicembre 2012 – 27 febbraio 2013, imp. Drummond et al. La sentenza è consultabile *on line* alla pagina *www.leggioggi.it/wp-content/uploads/2013/02/sentenza-google.pdf*.

35 Sullo sviluppo della controversia, fino al momento antecedente alla decisione della Corte di cassazione, v. E. APA – O. POLLICINO, *Modeling the Liability of Internet Service Providers: Google* vs *Vivi Down. A Constitutional Perspective*, Milano, Egea, 2013.

36 Il riferimento va, ovviamente, alla precitata direttiva 95/46/CE ed al d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

37 Cfr., in particolare, la direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»), recepita con il d.lgs. 9 aprile 2003, n. 70.

38 Corte di cassazione, sez. III pen., sentenza 3 febbraio 2014, n. 5107, cit., par. 7.1.

39 *Ibidem*.

40 *Ivi*, par. 7.2.

considerato quale titolare del trattamento, perché privo di qualsivoglia potere decisionale sul dato stesso»; «sono, dunque, gli utenti ad essere titolari del trattamento dei dati personali di terzi ospitati nei servizi di *hosting* e non i gestori che si limitano a fornire tali servizi»[41].

I principi posti hanno condotto alla assoluzione degli imputati, giacché «la posizione di Google Italia S.r.l. e dei suoi responsabili [era] quella di mero *Internet host provider*, soggetto che si limita[va] a fornire una piattaforma sulla quale gli utenti [potevano] liberamente caricare i loro video; video del cui contenuto resta[va]no gli esclusivi responsabili»[42].

Ora, comparando la posizione delineata per il motore di ricerca nelle due sentenze, emerge piuttosto chiaramente una discrasia, sulla scorta della quale, in un caso, al motore di ricerca si è imposto un *facere*, mentre, nell'altro, si è giustificata la sua posizione di neutralità apparente rispetto a contenuti che erano stati comunque trattati.

I due casi erano certamente diversi, lo si è premesso. E lo erano per l'organo giudicante, ma anche per il tipo di giudizio: non può escludersi, in specie, che l'atteggiamento più «liberale» espresso dalla Cassazione sia stato il frutto delle conseguenze su individui che la decisione del processo penale avrebbe potuto avere, conseguenze di sicuro più pesanti rispetto a quelle derivanti dalla statuizione della Corte di giustizia.

Resta il fatto, tuttavia, che una discrepanza si è effettivamente avuta, e che solo procedendo ad una eliminazione logica delle differenze tra le fattispecie si potrebbe addivenire a riconoscere nella sentenza successiva, resa a livello europeo, l'autorità di *leading case* generale per la materia. Un tale esercizio di armonizzazione, peraltro, dovrebbe fronteggiare un ulteriore ostacolo, di per sé idoneo a giustificare ciò che i giudici di *common law* definiscono «*distinguishing*»: nel caso originato in Spagna, i dati trattati provenivano da siti *web* per così dire «strutturati», mentre in quello italiano si trattava di *user generated contents*, cioè dei contenuti tipici dei *social media*.

Per questo aspetto, le due situazioni non appaiono, se non molto superficialmente, assimilabili, almeno sotto il profilo della protezione dei dati: da un lato, la presenza di informazioni personali sul sito di un quotidiano o di qualche altro soggetto implica che al titolare del sito si applichi la normativa sulla *privacy*, laddove un *user generated content* può essere inserito in una piattaforma *social* in cui il titolare dell'*account* agisca come persona fisica, non abbia fini commerciali, politici o filantropici, e magari consenta la condivisione ad un numero limitato o relativamente limitato di utenti, con il che si integrano pianamente le condizioni perché si dia luogo alla *household exemption*. Combinando questa differenza con gli esiti cui sono giunti le due sentenze, si arriva al paradosso per cui il *service provider* è titolare del trattamento di dati che provengono da soggetti a loro volta soggetti alla normativa sulla *privacy*, mentre non è da configurarsi come titolare del trattamento se ospita (ed indicizza) dati provenienti da soggetti non vincolati alla normativa. Si dirà che le tutele esistono comunque (e proprio il caso esaminato lo ha dimostrato[43]), ma ciò non impedisce di rimarcare l'anomalia degli esiti cui si addiviene.

Prendendo spunto dalla difformità riscontrata, qualche traccia di forzatura nell'assimilazione tra regime dei *social media* e diritto della rete in generale non può non essere evidenziata. Quando si pensa ai *social media*, infatti, si pensa soprattutto alla condivisione di contenuti tra soggetti che, nella stragrande maggioranza dei casi, sono persone fisiche cui si applica la *household exemption*: altrimenti detto, la normativa a tutela della *privacy* trova, nei *social*, un'applicazione tutto sommato marginale,

41 *Ibidem*.

42 *Ivi*, par. 8.

43 Uno dei procedimenti cui ha dato luogo la vicenda si è, infatti, concluso con la condanna degli studenti autori materiali dei maltrattamenti e del caricamento del video sulla piattaforma di condivisione.

potendo imporsi su chi gestisce la struttura (i *providers*), ma non su chi la frequenta (gli utenti). Alla luce di questa constatazione, la sensazione che sia agevole eludere le norme di protezione non può essere meramente epidermica: si pensi, ad esempio, al fatto che un contenuto ben può diventare «virale» semplicemente attraverso una catena di condivisioni fatte da soggetti che possono tutti appellarsi alla *household exemption*, con il che l'ipotetica violazione, anche grave, della *privacy* risulta essere il prodotto di una serie di azioni poste in essere di per sé in maniera legittima[44]. Se così è, allora diviene particolarmente importante la ricerca di forme di tutela che siano assicurate da altre normative: si giunge, per tal via, a doversi interrogare circa la reale efficacia nell'orientamento delle condotte poste in essere sui *social media* che può essere dispiegata dalla normativa generale suscettibile di avere per la *privacy* una portata protettiva, diretta o mediata.

5. Il parallelismo tra *social media* e mondo reale: l'omogeneizzazione forzata

La non perfetta corrispondenza – per usare un eufemismo – tra le norme generali a garanzia della *privacy* in rete e le esigenze che emergono dalle attività svolte nei *social media* evoca la necessità di valutare se, ed eventualmente in quale misura, l'ordinamento giuridico nel suo complesso possa comunque fornire risposte adeguate agli *inputs* di tutela emergenti nei e dai *social*.

La prassi giurisprudenziale degli ultimi anni parrebbe far propendere per una risposta generalmente affermativa: sono ormai cospicue nel numero le statuizioni che, da parte dei più diversi giudici, fanno applicazione, ad esempio, delle fattispecie penalistiche generali o delle tradizionali categorie del diritto privato alle condotte poste in essere *on line* dagli utenti di *social media*[45].

L'indicazione della prassi è, ovviamente, della massima importanza, tuttavia non pare di potersi escludere *a priori* la percorribilità di una lettura in certa parte diversa. Una lettura che prenda le mosse dall'assunto che la risposta che si richiede non è argomentabile in termini unicamente giuridici. La considerazione da parte del diritto di ciò che avviene sui *social media* dovrebbe, infatti, partire dalla constatazione della torsione che le relazioni *on line* assumono, rispetto allo *standard* rappresentato dalle relazioni del mondo reale, una torsione che si traduce, in estrema sintesi, nel naturale abbassamento delle tradizionali difese individuali nell'ambito delle relazioni sociali: l'espressione – in forma dialogica, di mera esternazione o anche nella versione quasi-meccanica della manifestazione di apprezzamento e/o condivisione di un messaggio[46] – segue procedimenti diversi a seconda che avvenga nella vita reale, di fronte ad altre persone, ovvero nel mondo virtuale, per il tramite di uno schermo che l'individuo gestisce isolatamente[47]. E questa diversità coinvolge, in primo luogo, proprio i meccanismi

44 Non a caso, in riferimento ai *social media*, si è espressamente parlato – in forma probabilmente iperbolica, ma non senza argomenti – de «la fine della *privacy*»: cfr. G. RIVA, *I social network*, cit., 147 ss.

45 Per una recente rassegna di giurisprudenza in materia, v. E. FALLETTI, *I* social network*: primi orientamenti giurisprudenziali*, in *Corriere giur.*, 2015, 992 ss. Con precipuo riferimento alla giurisprudenza relativa all'impatto dei *social media* sulla tutela della *privacy*, v. E. FERRARI, *I* social network*: la tutela della* privacy *nelle piazze virtuali*, in M. FUMAGALLI MERAVIGLIA (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica o scontro di civiltà?*, Napoli, Editoriale Scientifica, 2015, 139 ss.

46 «Visto dal lato dell'utente, la semplicità del meccanismo, che richiede nulla più che pigiare un pulsante, consente una partecipazione, in maniera rapida, alla vita sociale sul *social network*. Proprio la banalità del gesto, in molti casi, non consente di coglierne appieno ogni implicazione»: cfr. A.R. POPOLI, *Social network e concreta protezione dei dati sensibili*, cit., par. 3.8.

47 Le problematiche sociologiche legate ai *social media* sono esaminate da M. BOCCIA, *Sociologia dei new media*, in D.E. VIGANÒ (a cura di), *Dizionario della comunicazione*, Roma, Carocci, 2009, 652 ss. (*ivi* anche ulteriori riferimenti).

di difesa contro l'eccessiva estrinsecazione del proprio io[48]. Come è chiaro, su questo punto specifico la distanza tra mondo reale e mondo virtuale muta in misura assai rilevante a seconda del grado di cultura (informatica, ma non solo), di maturità, di consapevolezza del mezzo e della comunicazione. Le divaricazioni sono tanto marcate da rendere complicata finanche la formulazione di *standards* di attenzione, diligenza, etc. alla luce dei quali valutare i comportamenti tenuti sui *social*.

Questi rilievi hanno pesanti ricadute in termini giuridici, almeno sotto due punti di vista.

Innanzi tutto, la «spontaneità schermata» dei *social*, che si traduce nella suddetta discrepanza tra i comportamenti nel mondo reale e nel mondo virtuale, non può non produrre un qualche tipo di incidenza sulla valutazione *sub specie juris* delle condotte poste in essere. O, quanto meno, è presumibile che una qualche incidenza, molto spesso, sia opportuno che venga presa in considerazione. Con ciò si getta un'ombra piuttosto fitta sull'intero impianto normativo che, per come concretizzato dalla giurisprudenza, regge, attualmente, le relazioni sui *social media*. Altrimenti detto, se l'assenza di norme *ad hoc* ha portato *naturalmente* ad estendere ai *social*, per quanto possibile, i precetti che regolano i rapporti nella vita reale, non è dato cogliere da questa estensione *naturale* i segni dell'inevitabilità e, soprattutto, dell'opportunità scontata. Come si diceva, gli esempi che possono prospettarsi sono, ormai, molteplici; e non pochi riguardano, direttamente o in via mediata, proprio la *privacy*. Se si vanno ad analizzare alla luce del diverso approccio qui proposto, si può giungere alla conclusione che si tratta di esempi dai quali non emerge un compiuto parallelismo tra mondo reale e mondo virtuale; anzi, non è dato neppure individuare una corrispondenza in termini di entità del disvalore di certe condotte, poiché, a seconda dei casi, due azioni simili poste in essere l'una nel mondo reale e l'altra nel mondo virtuale possono colorarsi di un disvalore che è maggiore ora per l'una ora per l'altra.

Solo per prospettare un paio di casi, ovviamente senza alcuna pretesa di completezza, dai quali cogliere l'irriducibilità delle problematiche giuridiche sottese all'uso di *social media* da quelle tradizionalmente evocabili nel modo reale, può richiamarsi, in primo luogo, la contestazione del reato di sostituzione di persona, previsto all'art. 494 del Codice penale, a carico di chi crei un *account* su un *social network* utilizzando il nome di altri, inducendo così in errore i conoscenti della vittima, i quali si rapporteranno con il titolare dell'*account* fasullo come se fosse la persona da esso identificata[49]. Ora, il reato in questione, posto a tutela della fede pubblica, nella vita reale ha effetti che appaiono necessariamente più limitati di quelli cui può dar luogo una sostituzione di persona all'interno di un *social network*, e ciò per la semplice ragione che, una volta penetrato e diffuso nella *community*, l'*account*, dietro lo schermo della non verificabilità fisica dell'identità, è potenzialmente idoneo ad incidere su una serie indefinita ed ipoteticamente enorme di rapporti, veicolando informazioni personali (veritiere o false che siano) della vittima, ledendone l'immagine, etc., verso una platea di destinatari che può essere anche molto vasta, ed in ogni caso più vasta di quella che sembra essere suggerita dalla

48 In ordine all'impatto dei *social media* sui meccanismi cerebrali che guidano le relazioni sociali, v. G. RIVA, *Nativi digitali. Crescere e apprendere nel mondo nei nuovi media*, Bologna, il Mulino, 2014, spec. 67 ss.

49 Cfr., in part., Corte di cassazione, sezione V penale, 23 aprile – 16 giugno 2014), n. 25774, consultabile *on line* sul sito *Diritto penale contemporaneo* (*www.penalecontemporaneo.it/*), con il commento di F. SANSOBRINO, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona* (30 settembre 2014). Nella specie, l'imputato aveva «creato un profilo sul *social network Badoo* denominato "*Naty*", riproducente l'effige della persona offesa, con una descrizione tutt'altro che lusinghiera (ad esempio nelle informazioni personali era riportata la dicitura "*Mangio solo cibo spazzatura e bevo birra … quando mi ubriaco vado su di giri*") e con tale falsa identità usufruiva dei servizi del sito, consistenti essenzialmente nella possibilità di comunicazione in rete con gli altri iscritti (indotti in errore sulla sua identità) e di condivisione di contenuti (tra cui la stessa foto ritraente [la vittima del reato])».

previsione codicistica che punisce «chiunque […] induce *taluno* in errore».

Un esempio di segno opposto sembra che possa essere la qualificazione di un *post* inserito sulla bacheca di *Facebook* della persona offesa alla stregua di una diffamazione a mezzo stampa *ex* art. 595, terzo comma, del Codice penale, sulla base della potenzialità, della idoneità e della capacità del mezzo utilizzato di coinvolgere e raggiungere una pluralità di persone, non individuate specificamente[50]. Pur alla luce dell'interpretazione estensiva che della fattispecie incriminatrice è stata fatta, tale da ricomprendervi, tra le altre, le condotte diffamatorie poste in essere nel corso di comizi, non è forse compiutamente prospettabile una equiparazione tra un commento inserito su una bacheca di *Facebook* e quello contenuto – ad esempio – in un quotidiano, non fosse altro perché la diffusione del primo è più «controllabile», ma soprattutto è più facilmente individuabile e fronteggiabile in via autonoma da parte della vittima.

Rispetto al caso da ultimo prospettato, non è estranea la considerazione che proprio la «spontaneità schermata» che dei *social* è tipica può forse, se non giustificare, quanto meno attenuare la gravità, da un punto di vista soggettivo, della condotta posta in essere. Si arriva, in tal modo, al secondo elemento di criticità emergente dall'applicazione estensiva ai *social media* di norme concepite per tutt'altro *milieu*. Un mezzo di comunicazione basato, come sono i *social*, sull'istantaneità e sulla relativamente agevole possibilità di acquisire un *know-how* sufficiente ad un uso (magari nulla più che) rudimentale appare quanto mai insidioso per gli utenti, i quali sono portati a «socializzare» a prescindere dal reale controllo che possano mantenere sui loro dati e sulle loro azioni.

L'immagine ormai di uso comune della «piazza virtuale», oltre che metaforicamente accattivante, descrive in maniera abbastanza fedele l'idea di un aprirsi al pubblico che è insita nella – anzi, che è consustanziale alla – partecipazione ad un *social*. Il fatto è che la metafora regge nella parte in cui viene intesa in senso statico, cioè dello «stare in piazza», mentre appare fuorviante in un contesto dinamico, in cui, cioè, si prenda in considerazione anche l'azione anteriore, quella cioè dell'«andare in piazza»: in senso fisico, l'aprirsi al pubblico presuppone una serie di condotte che procedono da una determinazione in tal senso, si articolano in una serie di azioni materiali (prepararsi per uscire, uscire di casa, etc.), azioni che, non di rado, sono cadenzate da una progressiva apertura (ad esempio, l'uscita dall'appartamento implica i primi potenziali contatti con i condomini, cui seguono quelli con i vicini, fino a quelli con la moltitudine indistinta); l'accesso ai *social media*, invece, risponde a logiche di immediatezza assai più marcate, il che non può essere etichettato soltanto come un vantaggio in termini di risparmio di tempo, ma deve essere valutato anche in relazione alla imposizione di un adattamento repentino del registro comunicativo[51]. Un adattamento che non è scontato per alcuno, e che per talune categorie di soggetti (si pensi, in particolare, ai minori) è quanto meno problematico.

Il punto appare estremamente critico, perché revoca in dubbio le fondamenta stesse dell'equazione tra condotte poste in essere nel mondo reale e condotte nel mondo virtuale, non potendosi prescindere

50 In tal senso, v. Corte di cassazione, sezione I penale, sentenza 12 febbraio – 8 giugno 2015, n. 24431, consultabile *on line* sul sito *Altalex*, alla pagina *www.altalex.com/documents/news/2015/06/15/facebook-offesa-su-bacheca-diffamazione-a-mezzo-stampa*.

51 Implicazioni e conseguenze di queste difficoltà di adattamento sono riscontrabili in molteplici ambiti nei quali assumono una particolare delicatezza. Un esempio paradigmatico è quello del rapporto di lavoro, in relazione al quale i *social media* sono stati avvertiti come un possibile strumento di controllo da parte del datore di lavoro sui lavoratori meno attenti alla protezione dei loro dati. Per l'analisi di questa fattispecie, e di alcune delle pronunce emesse da giudici del lavoro in conseguenza di licenziamenti fondati su informazioni dal datore di lavoro acquisite (magari grazie a falsi profili) sui *social*, v. F. IAQUINTA – A. INGRAO, *La* privacy *e i dati sensibili del lavoratore legati all'utilizzo di* social networks*. Quando prevenire è meglio che curare*, in *Dir. relazioni industriali*, 2014, 1027 ss.; F. IAQUINTA – A. INGRAO, *Il datore di lavoro e l'inganno di* Facebook, in *Riv. it. dir. lav.*, 2015, 82 ss.

per queste ultime, almeno, dalla verifica della concreta capacità del soggetto di calarsi pienamente nel contesto in cui agisce. Ma, allora, l'assenza di una normazione specificamente rivolta alle azioni sui *social media* pone un'alternativa piuttosto netta tra l'ignorare semplicemente la discrasia che inficia l'equazione ed il rifarsi, di volta in volta, alla componente soggettiva che anima la condotta, il che significa, in ultima istanza, appellarsi alla responsabilità individuale.

Revocata in dubbio, sulla scorta di quanto fin qui detto, la validità della prima opzione, resta la seconda, sulla quale, peraltro, pure qualche riserva può formularsi, giacché affidare, per l'essenziale, alla responsabilità del singolo il suo «destino *social*» può risultare improprio, almeno in certi casi. Nel prosieguo si cercherà di dimostrarlo.

6. *Utens faber ipsius fortunae*: liberalismo o *Far West*?

È emblematico che, in un recente scritto dedicato alle norme che regolano i *social media*, si sia potuto candidamente affermare (o, forse meglio, amaramente constatare) che, «allo stato attuale dei fatti, la forma di protezione più efficace resta sempre l'autotutela, cioè la gestione attenta dei propri dati personali»[52]: come dire che l'aspirazione dei pubblici poteri a proteggere gli utenti, in questo caso, mostra tutta la sua debolezza, dovendo rivolgersi al decisivo apporto dato dalla responsabilità individuale.

Un tale affidamento potrebbe anche essere apprezzato, nel momento in cui se ne volesse mettere in risalto la matrice autenticamente umanistica riassumibile nell'affermazione per cui *homo faber ipsius fortunae*. Il problema, tuttavia, consiste proprio nella aleatorietà di tale affidamento, che è, per un verso, inattuale e, per l'altro, miope.

L'inattualità deriva dall'impossibilità di configurare l'utilizzo dei *social media* come un'attività così ordinaria che non si presti a disparità e ad abusi. Le questioni che l'accesso alla rete evoca, da sempre, in connessione con l'esistenza di divari digitali[53] non possono non essere trasposte, almeno *pro quota*, ai *social media*, relativamente ai quali il *quantum* di competenze informatiche è decisivo, non solo per l'accesso, ma – ed è questo l'aspetto che più interessa in questa sede – per il controllo sui contenuti immessi, nonché per il controllo, nei limiti del possibile, dei dati che siano da altri inseriti. Una pregiudiziale *no-regulation* dei *social media* assomiglia dunque molto, almeno allo stato attuale della diffusione degli strumenti informatici e delle relative conoscenze, ad un ponte verso un *Far West* virtuale, in cui – per giunta – a subire soprusi non sono solo i deboli che si scontrano con i forti, ma anche chi della comunità virtuale neppure fa parte (per qualunque motivo, magari soltanto per scelta) e che si trova alla mercé di qualunque *insider* e della sua attività comunicativa, che potrebbe riguardarlo.

Questa sensazione di inadeguatezza esce rafforzata in maniera significativa da quella che può definirsi come la «miopia» dell'atteggiamento eccessivamente liberale, che non tiene nel debito conto la prassi, troppo comune e diffusa per poter essere dissimulata dietro il velo di una falsa dichiarazione

52 Così, testualmente, E. FERRARI, *I* social network*: la tutela della* privacy *nelle piazze virtuali*, cit., 174.

53 Il tema è, come noto, tra i più studiati, specie da parte dei costituzionalisti. Tra i contributi più recenti, anche per gli opportuni approfondimenti bibliografici, v. P. COSTANZO, *Miti e realtà dell'accesso ad internet (una prospettiva costituzionalistica)*, in P. CARETTI (a cura di), *Studi in memoria di Paolo Barile*, Firenze, Passigli, 2013, 9 ss.; M. PETRANGELO, Oltre *l'accesso ad* Internet, *tra tutele formali ed interventi sostanziali. A proposito dell'attuazione del diritto di accesso ad* Internet, in M. NISTICÒ – P. PASSAGLIA (a cura di), Internet *e Costituzione*, Atti del Convegno. Pisa, 21-22 novembre 2013, Torino, Giappichelli, 2014, 169 ss.; L. NANNIPIERI, *La dimensione costituzionale del* digital divide*. In particolare, gli ostacoli cognitivi alla protezione dell'individuo nello spazio virtuale, ivi*, 189 ss.; P. OTRANTO, *Internet nell'organizzazione amministrativa: Reti di libertà*, Bari, Cacucci, 2015, 71 ss.

sull'età, che vede soggetti minori come utenti normalmente attivi (anzi, sovente iper-attivi) sui *social*[54].

Il regolamento euro-unitario non ignora questa tensione ideale, tanto che, al *considerando* 38, rimarca che «i minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali», ed ha cura di precisare che «tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di *marketing* o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore».

Questa preoccupazione si traduce nel divieto, posto dall'art. 8, par. 1, primo comma, di trattamento dei dati sulla base del consenso espresso da un minore di sedici anni (salvo il consenso del titolare della responsabilità genitoriale). La più che opportuna rigidità di questa disciplina si sgretola, tuttavia, già al secondo comma, allorché si consente agli Stati di derogare il limite anagrafico, purché non al di sotto dei tredici anni, età in relazione alla quale appare obiettivamente difficile poter presumere una – se non completa, almeno tendenziale – maturità; se, poi, si incrocia il dato normativo con i formulari contrattuali dei principali *social media*, la sensazione è che, nel regolare la materia, non si sia fatto altro che registrare una prassi, sull'assunto della inutilità di sforzi conformativi. Ancora più indicativo del grado di effettività che ci si possa attendere è quanto previsto dal par. 2 dell'art. 8, che, per il caso in cui sia richiesto, affida al titolare del trattamento il compito di «adopera[rsi] in ogni modo ragionevole per verificare […] che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili». Come dire che si chiede al controllato di mettere il controllore nelle condizioni di controllarlo.

Prescindendo dal coinvolgimento – più agevole da configurare in termini teorici che da strutturare in concreto – dei titolari della responsabilità genitoriale[55], l'affidamento alla responsabilità individuale appare, in effetti, difficile da giustificare allorché non si dia la possibilità neppure di stabilire una *fictio* di piena responsabilità, visto che ci si appella a soggetti che l'ordinamento è tenuto a proteggere in quanto incapaci.

La distanza tra *sein* e *sollen* emerge in maniera nitida allorché si vadano a ricercare gli interventi più significativi dell'Autorità Garante per la protezione dei dati personali italiana[56]. Come sottolineato nella relazione dalla stessa approntata per l'anno 2015, tra le attività di comunicazione ed informazione al pubblico figura quella di aver «fornito indicazioni per l'elaborazione di un sito informativo "Vivere in un mondo connesso" (*www.mondoconnesso.info*), realizzato da *Facebook* e lanciato anche in Germania, Austria e Francia, dedicato alla tutela dei dati personali su *internet* e nella vita quotidiana»: obiettivo del

54 Sulle problematiche connesse all'utilizzo dei *social* da parte dei minori ed alla loro tutela *on line*, v. L. MUSSELLI, *Internet e tutela dei minori*, in *Dir. informazione e informatica*, 2011, 727 ss.; L. MUSSELLI, *La tutela de minori nei nuovi media*, in R. CAFARI PANICO ET AL., *Da Internet ai Social Network*, cit., 57 ss. In una prospettiva più generale, v. G. DAMMACCO (a cura di), *Tutela giuridica del minore e uso consapevole di Internet*, Bari, Cacucci, 2008; F. PANUCCIO DATTOLA, *Minori e internet*, Torino, Giappichelli, 2009; A. THIENE, *L'inconsistente tutela dei minori nel mondo digitale*, in *Studium iuris*, 2012, 528 ss.

55 Interessante, in quest'ottica, è la sentenza resa dal Tribunale di Teramo il 16 gennaio 2012, n. 18, che, in una fattispecie di cyberbullismo, ha riscontrato la responsabilità dei genitori per il fatto del minore (anche qualora, come nella specie, prossimo alla maggiore età). Per il testo della decisione, v. M. BIANCA – A. GAMBINO – R. MESSINETTI (a cura di), *Libertà di manifestazione del pensiero e diritti fondamentali: profili applicativi nei social networks*, Milano, Giuffrè, 2016, 207 ss., con il commento di I. FAMULARO, *La responsabilità genitoriale per mancato controllo dei figli su Facebook*.

56 Per una sintesi dei vari interventi, a livello nazionale ed europeo, posti in essere nel quadro di una regolamentazione di *soft law* sui *social media*, v. P. GALDIERI, *Il trattamento illecito del dato nei* social network, in *Giur. merito*, 2012, 2697 ss.

sito, «corredato anche di uno strumento di autovalutazione delle competenze in materia di *privacy online* sviluppato da Unione nazionale consumatori», è quello «di raggiungere in maniera diretta gli utenti dei *social network* affinché prestino maggiore attenzione alla tutela della *privacy* in rete»[57]. Una iniziativa del genere appare, di per sé, come un'eloquente ammissione dell'insufficiente diffusione tra gli utenti delle competenze idonee ad una adeguata protezione della *privacy*.

Il Garante medesimo, del resto, allorché è intervenuto direttamente in materia, ha scelto uno strumento assai indicativo: un opuscolo informativo, una «guida ai *social network*», pubblicato nel 2009[58] e poi ripubblicato, in versione aggiornata, nel 2014[59], «con l'obiettivo di aumentare la consapevolezza degli utenti e offrire loro spunti di riflessione e strumenti di tutela»[60]. In concreto, tale opuscolo, dopo aver offerto cenni sulla nascita e la struttura dei *social networks* (non mancando di esplicitare i nomi dei più diffusi ed utilizzati)[61], si articola in una serie di «avvisi ai naviganti»[62] e di domande rivolte al lettore per stimolarne l'auto-responsabilizzazione («ti sei mai chiesto?»)[63], per poi formulare «10 consigli per non rimanere intrappolati»[64] e concludersi con un glossario dei principali termini gergali impiegati in rete[65].

Se questo opuscolo è stato pubblicato, oltretutto in due edizioni, è da presumersi che abbia una sua funzione ed utilità. L'estrema semplicità dei messaggi veicolati, però, fa pensare che, se una guida di tal fatta è utile, allora i suoi destinatari non devono essere particolarmente «esperti», quanto meno in riferimento alle implicazioni delle loro azioni sulla *privacy*. Ma, allora, l'affidarsi alla responsabilità individuale finisce per evocare alla mente lo stabilimento di una presunzione di dominio sul mezzo che l'utente medio dei *social media* in realtà non possiede.

In un quadro siffatto, sembra che ci si debba rassegnare ad appoggiarsi essenzialmente sui *service providers* perché agiscano, là dove possibile e nella misura in cui lo sia, a tutela degli utenti[66], mentre l'apparato pubblico si riserva una tutela strutturata sui normali canali, i quali – a fronte dell'immediatezza della rete (e dei *social* in special modo) – non consentono di configurare una tutela che non sia puramente successiva, una tutela, però, che proprio per il confronto impari rispetto alla velocità di trasmissione di messaggi, si presenta come inevitabilmente dimidiata.

Ciò equivale a dire che, per proteggere la *privacy*, l'alternativa è tra la tutela delegata a privati e la tutela pubblicistica che, come si diceva, è destinata ad arrivare tardi. Proprio come le forze dell'ordine

---

57 Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Relazione 2015*, 187. La relazione è consultabile *on line*, sul sito del Garante, alla pagina *http://194.242.234.211/documents/10160/5204506/Relazione+annuale+2015.pdf*.

58 V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Social Network: attenti agli effetti collaterali*, 2009, consultabile *on line* sul sito del Garante, alla pagina *http://194.242.234.211/documents/10160/10704/Opuscolo+Social+Network+pagina+singola.pdf*.

59 V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Social Privacy: come tutelarsi nell'era dei social network*, 2014, consultabile *on line* sul sito del Garante, alla pagina *http://194.242.234.211/documents/10160/2416443/Social+privacy.+Come+tutelarsi+nell%27era+dei+social+network.pdf*.

60 *Ivi*, 3.

61 *Ivi*, 5 ss.

62 *Ivi*, 9 ss.

63 *Ivi*, 17 ss.

64 *Ivi*, 23 ss.

65 *Ivi*, 31 ss.

66 Sullo spazio assunto dall'autoregolamentazione dei soggetti (e dei professionisti, *in primis*) nell'ambito delle comunicazioni elettroniche, v., anche per ulteriori riferimenti, S. VIGLIAR – V. VARRIALE – G. GIANNONE CODIGLIONE, *Le comunicazioni elettroniche*, in S. SICA – V. ZENO ZENCOVICH, *Manuale di diritto dell'informazione e della comunicazione*, 4ª ed., Padova, Wolters Kluwer-Cedam, 2015, spec. 359 ss.

nel *Far West*.

7. Qualche riflessione conclusiva su un possibile intervento della normativa di *hard law*

Le considerazioni da ultimo svolte inducono a concludere che i *social media* rappresentano, con ogni probabilità, il punto di caduta di tutte le costruzioni dalle quali emerge la difficoltà per il diritto di irreggimentare le relazioni sociali che dalla rete scaturiscono o che sulla rete si sviluppano. E, nelle pieghe di questa difficoltà, l'esigenza di regole (nel senso forte di *hard law*) non può non avvertirsi, almeno sotto alcuni punti di vista. Certo, la spinta in senso inverso non è da trascurare, specie quando fa leva sui pericoli di un controllo pubblico dai toni più o meno vagamente orwelliani. Non può ignorarsi, del resto, che la tentazione di «spegnere» i *social* è ricorrente in molti ordinamenti (specie, evidentemente, tra quelli che non si annoverano tra i «campioni» della liberal-democrazia): l'invocazione di un rafforzamento della tutela della *privacy*, in effetti, non si può escludere che mascheri intendimenti di compressione della libertà di espressione.

La ricerca di un bilanciamento tra le contrapposte esigenze è troppo complessa perché si possa ambire a percorrerla qui in un'ottica di ampio respiro. Non è detto, però, che interventi regolativi debbano necessariamente porsi nel solco di un siffatto bilanciamento: altre forme, meno impegnative, sono forse ipotizzabili, se non altro come rimedi parziali nei confronti di una situazione giuridicamente non soddisfacente. In particolare, non sembra escluso di poter associare al mantenimento degli attuali livelli di libertà nello «stare» all'interno della piazza virtuale, un incremento del tasso di regolamentazione della fase dinamica dell'accesso. In ordine all'attività posta in essere sui *social media* una disciplina è rintracciabile; e, per quanto le soluzioni da essa offerte non risultino invariabilmente soddisfacenti, prospettare una rivisitazione *ab imis* implicherebbe il prendere posizione su tematiche di estrema delicatezza, tanto da non potersi escludere l'eventualità di giungere ad una situazione finale non significativamente migliore rispetto a quella presente; una tale constatazione non pare che debba estendersi anche alla fase dell'accesso sui *social*, giacché in essa si manifestano elementi che si presentano fortemente tipizzanti, al punto da consentire (e rendere opportuna) una considerazione specifica. Per dirla in termini forse più concreti, se – pur con le molte riserve che si sono sopra accennate – può considerarsi non insostenibile, almeno in linea tendenziale, una applicazione estensiva (o, meglio, analogica) all'attività svolta sui *social media* delle disposizioni che regolano le attività del mondo reale e/o delle normative generali previste per il mondo della rete, non altrettanto pare che possa dirsi per la disciplina del momento in cui ai *social* si accede, ed in particolare del momento della registrazione.

La registrazione rappresenta, in effetti, una fase di estrema importanza, non solo per l'ovvia ragione che apre al singolo le porte della «piazza virtuale», ma anche perché è in quel frangente che sarebbe possibile porre davvero un diaframma contro accessi inopportuni o non sufficientemente consapevoli. L'utilizzo del condizionale è d'obbligo, se non altro per ciò che si è detto in precedenza sulla non controllabilità dell'accesso da parte dei minori.

Ma c'è anche un'altra ragione che spiega l'uso del modo verbale. Generalmente, l'attenzione viene posta su *chi* accede, il che comporta che il sistema normativo si interessi essenzialmente di vietare l'accesso a chi non ne abbia astrattamente titolo (in quanto al di sotto di una certa soglia anagrafica). Ne discende un sistema non troppo dissimile da un insieme di grida manzoniane, come dimostrato dalla sopra ricordata normativa del regolamento euro-unitario sul controllo del rispetto dei divieti. Non si vuol certo prospettare l'inutilità di siffatte previsioni, le quali debbono, ovviamente, esserci, ed anzi si dovrebbe trovare il modo di renderle quanto più efficaci possibile. Ma non dovrebbero esserci soltanto

queste: una regolamentazione di *hard law* non dovrebbe trascurare il *come* si accede, perché è nella disciplina di quel procedimento che si possono porre le basi per un accesso *consapevole* ai *social media*. In sostanza, una normativa, specie se europea, che specificasse in forma compiuta le modalità attraverso cui registrarsi potrebbe imporre ai *service providers* oneri legati alla conoscibilità reale di ciò che accedere al servizio significa, anche e soprattutto in termini di *privacy*, *sub specie* di trattamento dei dati, sia da parte del fornitore che da quella dell'utente (per i dati propri e per quelli altrui). La inevitabile compressione della libertà contrattuale risulterebbe, in quest'ottica, giustificabile in relazione alla protezione di altri principi ed esigenze, di sicuro rilievo costituzionale; senza contare che si tradurrebbe comunque in una compressione apprezzabile in relazione ad un singolo momento e limitatamente alle forme attraverso cui esprimere i contenuti contrattuali che già oggi sono individuabili.

L'attuale carenza di una normativa che ambisca a razionalizzare la prassi estremamente variegata dei singoli *social media* ha creato una situazione in cui il rispetto del (puro) formalismo finisce per essere qualcosa di non troppo dissimile da un «guscio vuoto»[67]. Al potenziale utente si chiede di compilare campi e di accettare condizioni, per lo più nella forma – tanto snella quanto sfuggente – del *point and click*[68]. Campi e condizioni che sono di problematica intelligibilità finanche per il giurista, e ciò non solo per il dettaglio delle specificazioni tecniche, ma anche per la formulazione stessa del contratto, che talora, ad esempio, segue stili discorsivi in cui la portata precettiva degli obblighi tende a diluirsi. Per tacere delle soluzioni non sempre di immediata evidenza relative al diritto applicabile in caso di controversia e del relativo foro competente, e di molte altre clausole di tenore e portata assai ondivaghi[69]. A complicare il tutto, si pongono poi le incertezze connesse all'uso di più lingue, ferma restando però l'ufficialità del solo inglese, donde la necessità di sommare a cospicue competenze giuridiche solide basi linguistiche.

Ora, per come la trama normativa si è evoluta, l'intelligibilità è divenuta inversamente proporzionale all'entità degli obblighi imposti ai *providers*, le cui *privacy policies* sono chiaramente ispirate all'adempimento di obblighi di mezzo, dove il risultato resta, nel migliore dei casi, sullo sfondo[70]. Il chiedere ai *providers* di inserire questo o quel contenuto, di per sé, non è risolutivo, se non lo si collega ad un obbligo di estrinsecare questi contenuti in forme che possano essere effettivamente percepite dall'utente medio. Il paradosso che ne discende è che solo imponendo un obbligo puramente strumentale (consistente nel *quomodo* dell'esposizione dei contenuti) si può ambire ad un grado accettabile di raggiungimento di un obbligo di risultato (*id est*, l'effettiva consapevolezza da parte dell'utente del tipo di accordo che va stipulando).

Un mutamento di approccio nel senso qui auspicato non costituirebbe – è chiaro – *la* soluzione delle difficoltà che si riscontrano nella disciplina dei *social media*; sarebbe, tuttavia, un passo significativo, sia per i suoi auspicabili effetti concreti, sia (forse soprattutto) per il senso che l'intervento potrebbe

67 Una efficace rassegna critica delle modalità attraverso cui il potenziale utente può registrarsi alle varie piattaforme *social* è condotta da A.R. POPOLI, *Social network e concreta protezione dei dati sensibili*, cit., parr. 3. ss.

68 È appena il caso di rilevare che la critica di cui nel testo non è diretta a contestare la validità in sé dei contratti conclusi per il tramite di questa formalità (sebbene in proposito non siano prive di argomenti le tesi, autorevolmente sostenute, che avanzano dubbi di legittimità: cfr., in part., N. IRTI, *Scambi senza accordo*, in *Riv. trim. dir. proc. civ*., 1998, 347 ss.), ma è semplicemente rivolta a mettere in rilievo gli effetti potenzialmente pregiudizievoli derivanti da contratti conclusi con eccessiva facilità.

69 Per una rassegna compiuta delle problematiche che emergono dalle *privacy policies*, v., di nuovo, A.R. POPOLI, *Social network e concreta protezione dei dati sensibili*, cit., parr. 3.3. ss.

70 Con riferimento all'effettività della prestazione del consenso da parte degli utenti della rete, v., da ultima, S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e dir. priv.*, 2016, 513 ss., che pone in particolare risalto la transizione da un «libero consenso informato» ad un «consenso disinteressato».

testimoniare, e cioè quello di operare una saldatura tra un *hard law* a lungo latitante e l'azione principalmente pedagogica che è stata perseguita dalle linee-guida adottate negli anni da organi operanti nel settore ai più vari (ed anche ai massimi) livelli. Il che equivarrebbe, in buona sostanza, ad argomentare che, là dove veramente è necessario, le istituzioni politiche sono in grado di imporre propri *standards*, volti ad evitare che la tutela della libertà (contrattuale, *avant tout*) non si traduca in una preconcetta accettazione di uno stato di quasi-anomia. Come dire che, anche in un ambito in cui si è finora mosso con estrema circospezione, l'*hard law* si riserva di intervenire per garantire le basi di una ordinata convivenza, anche virtuale.