UNIVERSITÀ DEGLI STUDI DI MILANO BICOCCA

DIPARTIMENTO DEI SISTEMI GIURIDICI ED ECONOMICI

DOTTORATO DI RICERCA IN SCIENZE GIURIDICHE

CURRICULUM 14: FILOSOFIA E SOCIOLOGIA DEL DIRITTO (IUS 20)
XXIV CICLO

Anno accademico 2012/2013

IL GLOBAL PRIVACY STANDARD:
I MODELLI DI TUTELA DELLA PRIVACY

TUTOR: PROF. ANDREA ROSSETTI

TESI DI DOTTORATO DI
STEFANO RICCI

INDICE

Premessa.

La tesi che propongo segue uno sviluppo descrittivo che mira ad illustrare e catalogare progressivamente le varie concezioni della privacy. L'analisi (identificazione, distinzione e classificazione dei concetti) è finalizzata a mettere a fuoco i molteplici significati della parola "privacy" procedendo in forma circolare e non lineare.

Si tratta dunque di catalogare le varie concezioni anzitutto identificandole, distinguendole e ponendo in rilievo le sovrapposizioni concettuali e regolative (quel che definiamo modello di tutela).

Nella prima parte distingueremo quindi il diritto alla protezione dei dati personali dal diritto alla riservatezza, e il diritto alla privacy (che li ricomprende entrambi) dalla privacy come valore. Tale distinzione ci consente di illuminare due valori fondamentali: la libertà negativa (intimità) e la libertà positiva (identità). L'assunto è che la comprensione dei diversi valori in gioco conduce ad una migliore comprensione dei modelli di tutela, ossia delle regole che sono poste a loro tutela. Premesso che i valori non esistono in sé ma esistono oggetti (sociali) cui attribuiamo valore perché soddisfano i nostri bisogni, constatiamo che la privacy come valore soddisfa il nostro bisogno di libertà, sia negativa sia positiva.

Al fine di meglio connotare questa differenza tra libertà negativa e libertà positiva per quanto qui ci interessa, sosteniamo che la privacy come libertà negativa sia una forma di intimità e la privacy come libertà positiva sia una forma di identità, vale a dire che il concetto di privacy come libertà negativa si sovrappone ma non si esaurisce in quello di intimità e lo stesso dicasi per il concetto di privacy come libertà positiva rispetto a quello

di identità; tuttavia intimità e identità consentono di meglio distinguere i valori che sono perseguiti dalle regole sulla privacy: esistono quindi regole a tutela dell'intimità, o privacy come libertà negativa, e regole a tutela dell'identità, o privacy come libertà positiva.

Procedendo nel secondo capitolo all'illustrazione dei vari modelli di tutela, osserveremo che la privacy come diritto è la pretesa che altri facciano o non facciano qualcosa riguardante i nostri fatti privati e i nostri dati personali. Pretendiamo che non si pubblichino quelle foto e pretendiamo che si cancellino quelle informazioni. Questa prima distinzione (fatti privati/dati personali) è un primo indizio che ci induce a rendere conto di almeno due forme di privacy come diritto: regole a tutela dell'intimità (fatti privati) e regole a tutela dell'identità (dati personali). Vedremo quindi che nel primo caso avremo essenzialmente regole di opacità in base ad un interesse a celare aspetti ed informazioni attinenti la nostra vita e nel secondo caso regole di trasparenza volte a chiarire entro quale ambito certe informazioni possono essere condivise. Elencheremo vari modelli di tutela: la *privacy as dignity* (a tutela dell'intimità), la *privacy as property* (a tutela dell'intimità), la *privacy as (new) confidentiality* (a tutela dell'identità) e la *privacy as copyright* (a tutela dell'identità).

La privacy è la totalità di questi concetti e di questi modelli di tutela. A fronte di questa totalità, nella terza parte, si offre una nuova tassonomia basata su tre rapporti giuridici fondamentali: tra interessato (lo chiameremo *data subject*) e gestore della banca dati (lo chiameremo *data holder*); tra interessato e contro interessato (lo chiameremo *stakeholder*); tra *data holder* e *stakeholder* in relazione alle informazioni riguardanti il *data subject*. L'insieme dei principi e delle regole che viene definito Global Privacy

Standard riguarda solo il primo rapporto e deve essere rimodulato in relazione al valore che intende realizzare, ossia quello di identità contestuale. Pertanto il miglior modello di tutela, a nostro modo di vedere, è quello di confidenzialità opportunamente adattato al nuovo contesto digitale.

CAPITOLO I – LA PRIVACY QUALE VALORE

1. Privacy e libertà

Di che cosa parliamo quando parliamo di privacy? Che cosa si intende per Global Privacy Standard? Nell'espressione "Global Privacy Standard" il termine standard, usato in particolare in ambito ingegneristico o informatico, si riferisce all'insieme delle norme – stabilite convenzionalmente o imposte dall'autorità – che hanno lo scopo di rappresentare la base di riferimento per la realizzazione di tecnologie tra loro compatibili e interoperabili. Quando si parla di standard globali in materia di privacy ci si riferisce alle norme che hanno lo scopo di consentire la circolazione dei dati personali, ossia riferibili a un soggetto, sia esso identificato o identificabile. Per dato s'intende[1] qualsiasi rappresentazione di fatti, informazioni o concetti; mentre il dato informatico, più specificamente, è qualsiasi dato che può essere trattato da un sistema di informazione, compreso un programma atto a far svolgere una funzione ad un sistema di informazione. La disciplina giuridica che si occupa del trattamento e della circolazione dei dati personali viene anche definita protezione dei dati personali (o "*data protection*").

Tuttavia, diritto alla privacy e *data protection* sono termini giuridici non completamente sovrapponibili: la protezione dei dati personali non riguarda necessariamente la tutela della vita privata, essendo il suo oggetto di tutela

[1] Vedi la Decisione quadro del Consiglio dell'Unione europea del 24 febbraio 2005, n. 2005/222/GAI.

il dato personale, ossia quell'informazione che riguarda una persona identificata o identificabile.

Da una parte, infatti, il dato privato è qualcosa che è caratterizzato da un certo statuto d'inaccessibilità e/o indisponibilità per i terzi a tutela di una dimensione intima del soggetto; dall'altro lato, il dato personale è quell'informazione che consente l'identificazione di un soggetto, ossia la possibilità di distinguere un individuo da tutti gli altri attraverso il riferimento ad alcuni dati. L'insieme di dati riferiti a quell'individuo rappresenta la sua identità[2].

Oggi con il termine privacy ci riferiamo sia alla tutela accordata dall'ordinamento a una dimensione della nostra vita, la sfera privata (o intima), che resta o dovrebbe restare inaccessibile a terzi[3] sia alla possibilità di controllare[4] i dati personali che costituiscono la nostra

---

[2] Il termine "identità" si riferisce all'insieme dei dati che, da un lato, identificano uno specifico individuo rispetto agli altri e, dall'altro, ne connotano altri aspetti o altre caratteristiche in vari ambiti della vita di relazione: la terminologia della *data protection* parla di dati personali identificativi, da un lato, e dati personali non identificativi, dall'altro. Si potrebbe quindi correttamente distinguere tra identità ed identificazione e affermare che la *data protection* disciplina la possibilità per chi gestisce una banca dati, una volta legittimamente identificato l'individuo, di trattare i suoi dati, lasciandogli in ogni caso il potere di controllarne tale uso. In termini analoghi: Alan F. Westin, *Privacy and freedom*, in *New York: Athenum*, 1967, p. 31.

[3] David Lyon, *La società sorvegliata tecnologie di controllo della vita quotidiana*, Milano, 2003 p. 9; Hannah Arendt, *Vita activa*, Milano, 2009, p. 28.

[4] La definizione più nota a livello internazionale del diritto alla privacy ne è un esempio: per Alan Westin la privacy è "*la pretesa di individui, gruppi o istituzioni di decidere autonomamente*

identità. I modelli di tutela della sfera privata individuale e dell'identità personale, però, non sempre coincidono.

Tuttavia avremo modo di verificare che entrambi questi valori sono legati a particolari contesti.

La dicotomia pubblico/privato[5] delinea per l'appunto contesti diversi, il primo ad accessibilità generale (pubblico) ed il secondo ad accessibilità limitata (privato); lo statuto di una particolare informazione, quindi, dipende dal contesto, pubblico e privato, che le è riconosciuto dalle norme sociali e giuridiche. Le vicende di ambito familiare, così come le condotte individuali o sociali che si svolgono in luoghi quali la propria casa, sono tradizionalmente considerate non accessibili alla generalità delle persone. Si tratta di una prima forma di privacy basilare che possiamo definire *spatial privacy*[6]. Esistono degli spazi privati: ciò che avviene entro questi spazi gode di uno statuto di limitata accessibilità per i terzi. In parallelo, ciò che avviene in uno spazio pubblico, come un parco, è immediatamente accessibile a chiunque. Analogamente: quando si parla di conversazioni private ci riferiamo al fatto che il contenuto delle nostre comunicazioni dovrebbe

---

quando, come e in quale misura le informazioni su di loro vengono comunicate agli altri": vedi Alan F. Westin, cit.

[5] Helen Nissenbaum, *Privacy as contextual integrity*, in *Washington Law Review*, 2004, p. 119 e ss.; Lisa Austin, *Privacy and the Question of Technology*, in *Law and Philosophy*, 2003, p. 120; Neil M. Richards, *The limits of tort privacy*, in *Journal on Telecommunication & High Technology Law*, 2011, p. 363.

[6] Gavison Ruth, *Privacy and the Limits of Law*, in *Yale Law Journal*, 1980, p. 424; Daniel Solove, *No privacy*, Milano, 2009, p. 174 e ss.; Helen Nissenbaum, cit., p. 115 e 124 e ss.; Neil M. Richards, *Intellectual privacy*, in *Texas Law Review*, 2008, p. 412; vedi anche Neil M. Richards, *The limits of tort privacy*, cit., p. 384.

essere inaccessibile ai terzi[7]. Quando ciò non accade, si ha una violazione della privacy. Parliamo quindi non solo di spazi privati ma più genericamente di contesti privati.

Allo stesso modo, in materia di *data protection*, la circolazione delle informazioni che ci riguardano (i nostri dati personali) è legata al particolare contesto in cui le informazioni vengono scambiate. Soltanto che non è sempre rilevante il contesto pubblico e privato, quanto piuttosto il contesto relazionale entro cui avviene il trasferimento di informazioni: al momento dell'acquisto di un biglietto aereo, sarà del tutto normale fornire le informazioni legate alla mia identità di viaggiatore, ossia nome, cognome, dettagli del documento di riconoscimento, destinazione del viaggio e così via. Sarà invece anomalo che mi si chieda, magari per ragioni di sicurezza, lo scopo del viaggio o, a maggior ragione, le persone con cui ho intenzione di incontrarmi. Il contesto ed il tipo di relazione determinano quali informazioni, personali e non, è ammissibile che vengano scambiate senza che il soggetto senta di subire un'invasione nella propria privacy[8]. Parliamo quindi di contesti relazionali.

Sotto il profilo terminologico, se la *data protection* è l'insieme delle regole per il (corretto) trattamento delle informazioni personali, il diritto alla privacy è qualcosa di più ampio: la *data protection* ne è quindi un sotto insieme, nel momento in cui viene definita come la pretesa di controllo su quelle informazioni[9]: una prova evidente è che

---

[7] Il problema, che non possiamo affrontare in questa sede, è della corretta identificazione del soggetto "terzo".

[8] Helen Nissenbaum, cit., p. 119.

[9] La già citata definizione di Westin. Vedi anche Charles Fried, *Privacy*, in *Yale Law Journal*, 1968, p. 475; per altri riferimenti cfr. Lisa Austin, cit., p. 123.

il Decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, viene comunemente definito come Codice Privacy. Altro sotto insieme è quello che potremo definire quale diritto alla riservatezza, ossia l'insieme degli strumenti di tutela della vita privata dell'individuo (dei suoi contesti privati): le norme costituzionali che limitano il potere dello Stato di compiere ispezioni, sequestri e intercettazioni di comunicazioni; le norme penali che puniscono la violazione di domicilio, l'accesso abusivo a sistema informatico, l'interferenza illecita nella vita privata altrui, la sottrazione o presa di cognizione della corrispondenza; le norme civili che impediscono la pubblicazione di fatti privati e in caso di violazione impongono il risarcimento dei danni.

Per chiarire questa distinzione riteniamo utile spostare il livello della nostra analisi sulla privacy come valore. Dobbiamo partire dal presupposto che, quando parliamo comunemente di privacy, ci riferiamo indistintamente alla privacy come diritto e alla privacy come valore e ciò può facilmente generare confusione. Il valore della privacy[10] chiarisce ciò che è il diritto alla privacy e ci permette un miglior bilanciamento con eventuali beni in conflitto.

Vi sono due valori[11] fondamentali legati alla privacy:

---

[10] Daniel Solove, *Conceptualizing privacy*, in *California Law Review*, 2002, p. 1143; Gavison Ruth, *Privacy and the Limits of Law*, in *Yale Law Journal*, 1980, p. 428 e ss.

[11] La distinzione tra diritto e valore è analoga a quello tra strumento e fine: non esistono propriamente valori ma cose a cui viene attribuito un valore. Ciò rappresenta il fine di un certo modello normativo, strumento di attuazione di quel fine. Quel che definiamo valore è pertanto esemplificazione di una qualità, sorta

una dimensione di libertà[12] in senso negativo che delinea una sfera limitatamente accessibile da parte di terzi e che possiamo anche definire privacy come intimità[13] – *privacy as intimacy* – e una dimensione di controllo sui dati personali che riguardano il soggetto, ossia il controllo[14] sulle informazioni riguardanti se stessi e quindi sulla propria identità in quanto individuo (libertà in senso positivo ovvero privacy come identità – *privacy as identity*).

Focalizziamo la distinzione tra i due valori della privacy che abbiamo individuato. La privacy come libertà negativa è una sfera entro cui è possibile fare scelte e tenere comportamenti al riparo dagli altri: è dunque una libertà di agire; la privacy come libertà positiva non è il mero rispetto di questa sfera: è, piuttosto, una forma di

---

per astrazione dal mondo delle nostre esigenze, che funge da criterio per le nostre scelte e per valutare le scelte altrui. Norberto Bobbio, *Introduzione alla filosofia del diritto*, 1948, Torino, p. 36 e ss.

[12] Il punto di riferimento è ovviamente l'opera di Berlin. Isaiah Berlin, *Libertà*, Milano, 2002 e di Norberto Bobbio, *Eguaglianza e libertà*, Torino, 1995, p. 45 e ss.; il rapporto tra privacy e libertà è stato più volte messo in luce da vari autori: Wolfgang Sofsky, *In difesa del privato*, Torino, 2007, p. 15; Lisa Austin, cit., p. 147; Helen Nissenbaum, cit., p. 130.

[13] Thomas Nagel, *Concealment and Exposure*, in *Oxford University Press*, 2002, p. 4; Daniel Solove, *Conceptualizing privacy*, cit., p. 1121.

[14] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, Milano, 2010, p. 118 e 120: "è il diritto decidere innanzitutto *come* – e non tanto *se* – partecipare alla condivisione delle informazioni"; vedi anche Stefano Rodotà, *La vita e le regole*, Milano, 2009, p. 100 e ss. e Julie E. Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*, in *Yale University Press*, 2012, p. 135.

autodeterminazione riguardante le informazioni su di sè. Questa libertà positiva deriva dal desiderio dell'individuo di essere padrone delle proprie informazioni e di determinare così la propria identità nella sfera pubblica.

Queste due forme di libertà hanno avuto origine, sviluppo e modello di tutela differenti, tanto è vero che per fare chiarezza terminologica sarebbe bene riservare il termine privacy solo alla libertà in forma negativa (l'abbiamo definita *privacy as intimacy*, o *hard privacy*) e utilizzare un termine diverso per l'autodeterminazione sulle proprie informazioni (l'abbiamo definita *privacy as identity*, o *soft privacy*). Da un lato, quindi, la possibilità di agire al riparo da intrusioni ed ingerenze di terzi; dall'altro, la possibilità di controllare le proprie informazioni e plasmare la propria identità.

In ogni caso, nella letteratura scientifica il termine privacy (come valore) fa riferimento sia alla libertà di agire indisturbati sia all'autonomia nel controllo dei dati personali riferiti a se stessi. Ciò, purtroppo, non fa che rendere incerte le regole concretamente applicabili ai casi controversi. Un esempio è la disciplina dell'attività giornalistica e lo scontro tra libertà di informazione e diritto alla privacy inteso quale controllo sulle proprie informazioni personali (a tutela quindi dell'identità personale dell'interessato).

Continuando a utilizzare la terminologia di Isaiah Berlin[15], la privacy è una particolare forma di libertà (vedi anche la Convenzione di Strasburgo 28 gennaio 1981 che la qualifica "*fundamental freedom*") che si concreta nella possibilità di sottrarsi dalla sfera pubblica, cioè di agire liberi da interferenze (per tale ragione ci riferiamo ad essa

[15] Isaiah Berlin, *Libertà*, cit.

come libertà negativa)[16]; è altresì ricompresa nell'alveo del concetto di privacy l'autodeterminazione informativa, vale a dire la possibilità di scegliere quali informazioni riguardanti la propria persona far circolare nella sfera pubblica (libertà positiva). Quello che cercheremo di mostrare è che la privacy come libertà negativa riguarda la tutela di particolari contesti privati, così qualificati da norme giuridiche e sociali, nel quale si svolgono determinate attività. La privacy come libertà positiva non riguarda più la dicotomia pubblico/privato (e quindi il contesto pubblico e quello privato) ma si sostanzia piuttosto nella tutela delle nostra identità in un determinato contesto in cui la qualificazione di pubblico e privato perde centralità ed è per questa ragione che preferiamo usare il sintagma identità contestuale, da intendersi come l'insieme degli attributi non mutevoli di un individuo in un determinato contesto relazionale e sociale (*privacy as contextual identity*).

2. Pubblico e privato

Per poter procedere nell'analisi, occorre definire cosa si intende per pubblico e per privato, dal momento che la privacy quale libertà negativa si fonda su tale distinzione.

Pubblico (da *poplicus*, contrazione di *popolicus*, che sta per *popolus*) ha tre significati principali: concretamente, ciò che è accessibile o esposto a tutti (al *popolus*, ossia alla collettività, ad esempio nelle espressioni "luogo pubblico", "luogo aperto al pubblico" o "luogo esposto al pubblico"); più astrattamente e

[16] John Rawls, *Lezioni di storia della filosofia politica*, Milano, 2009, p. 102.

genericamente, ciò che riguarda e pertiene tutta la collettività (ad esempio nel sintagma "interesse pubblico"); infine ciò che è espressione o appartiene all'ipostatizzazione dell'idea di popolo, ossia allo Stato-apparato (ad es. quando si legge della "funzione pubblica" o di un "bene pubblico").

Il "pubblico", così definito, ha, quindi, un nucleo di significato essenziale che sta per generalmente "accessibile" e un'ulteriore area semantica che sta per "pertinente" (i) alla comunità-popolo in quanto tale (useremo, per evitare incomprensioni e per riferirci più precisamente a questa accezione, il termine "collettivo") oppure (ii) alla comunità-istituzione che è lo Stato (useremo, qui, il termine "statuale"). È molto importante tenere distinto il "pubblico in senso collettivo" e il "pubblico in senso statuale"[17]. Avremo modo di verificare, infatti, che il modello di tutela dei contesti privati rispetto ad ingerenze statuali è diverso dal modello di tutela riscontrabile in presenza di interessi pubblici collettivi. Ci si riferisce al termine "pubblico" in senso collettivo, ad esempio, quando si parla d'interesse pubblico alla conoscenza di un'informazione o all'espressione della libertà di manifestazione del pensiero. Ciascun membro della collettività è portatore di quell'interesse, interesse che magari si trova in netto contrasto con ulteriori interessi dello Stato-apparato. Si parla di "pubblico" in senso statuale, invece, quando si cita, ad esempio, l'interesse pubblico a preservare la sicurezza nazionale oppure

[17] La distinzione si rinviene anche in Hannah Arendt, cit., p. 28 e ss. quando teorizza la distinzione tra sfera pubblica (e politica) e sfera sociale, entrambe contrapposte alla sfera privata dell'individuo; per una distinzione tra sovrano e collettività nella tradizione liberale vedi John Rawls, cit., p. 80 e ss.

all'accertamento e alla repressione dei reati attraverso l'uso della forza[18]: tale interesse appartiene senza dubbio anche a ciascun membro della collettività ma il compito è stato delegato, nelle forme della democrazia rappresentativa, allo Stato-apparato che deve darne attuazione. È importante sottolineare sin d'ora che la sfera privata viene delimitata sia dalla sfera pubblica collettiva, cioè dalle posizioni giuridiche di soggetti, individuali e non, di pari livello dell'interessato - la definiremo, perciò, privacy orizzontale - sia dalla sfera pubblica statuale, ovvero dal potere proveniente dall'autorità sovraindividuale - per tale ragione si parlerà di privacy verticale -. La tradizione giuridica si è soffermata più su quest'ultima (cosiddetta *constitutional privacy*, vale a dire l'insieme dei principi volti a limitare il potere dell'autorità statuale) ma, ad esempio, la nascita del diritto alla privacy è collegata alla pubblicazione di foto private da parte della stampa (cosiddetta *tort privacy,* perché riconosceva un diritto d'azione dell'individuo contro il giornale che aveva pubblicato foto indiscrete).

Quando si legge che "il buon giornalismo sa che i fatti non sono mai al sicuro nelle mani del potere e se ne fa custode nell'interesse dell'opinione pubblica" (la frase è di Giuseppe D'Avanzo), si contrappone il potere pubblico (statuale) all'opinione pubblica (collettiva), ossia l'apparato alla comunità; tale distinzione corrisponde alla ben nota differenza[19] tra Stato-apparato (pubblico statuale) e Stato-comunità (pubblico collettivo). Molto spesso queste due accezioni vengono confuse, più o meno consapevolmente. Affermare che un bene è pubblico

[18] Helen Nissenbaum, cit., p. 107.
[19] Aljs Vignudelli, *Diritto costituzionale*, Torino, 2010, p. 129.

sembra evocare che quel bene appartenga alla collettività: in realtà il diritto di proprietà è esercitato dallo Stato-apparato, non certo dallo Stato-comunità. In ogni caso, sia lo Stato-apparato (pubblico statuale) sia lo Stato-comunità (pubblico collettivo) possono rappresentare una minaccia per la privacy dell'individuo, concetto che, nella sua accezione moderna, mostra chiaramente il segno della sua matrice filosofica liberale.

Il termine privacy deriva dal latino *privatu(m)*, che a sua volta deriva da *privu(m)* cioè "che sta davanti, isolato"; attestato in inglese in senso generico dal 1450 circa e nel senso specifico "la vita privata di ciascuno e la relativa riservatezza" dal 1814, è stato introdotto in italiano nel 1951 (in un articolo comparso nel settimanale "Epoca" del 7 luglio dello stesso anno)[20]. Privato è, quindi, un attributo che rimanda immediatamente ad una sottrazione[21], consistente nella restrizione della possibilità, fattuale o normativa, di accesso da parte di altri al sostantivo cui si riferisce (ad esempio nelle espressioni "un'informazione privata" o "una conversazione privata" – ci si riferisce ad un'informazione cui i terzi non possono avere accesso). Quale contrario di "pubblico", conserva anche il significato di pertinente ad un individuo contrapposto tanto alla collettività che allo Stato. La privatezza è, dunque, quella particolare dimensione dell'individuo, non accessibile agli altri o comunque interdetta alla generalità degli altri consociati. Abbiamo già considerato che la privatezza si realizza in determinati contesti che sono tradizionalmente considerati privati: la vita familiare, il

[20] Come spiega il *Dizionario Etimologico della Lingua Italiana* (comunemente abbreviato in DELI) di Manlio Cortelazzo e Paolo Zolli - B. Mortara Garavelli, *La Crusca per voi*, n. 25.
[21] Hannah Arendt, cit., p. 28.

proprio domicilio, le comunicazioni (*spatial privacy*). Tuttavia, non sempre lo statuto di limitata accessibilità e disponibilità è collegato ad uno dei sopra richiamati contesti privati. Vi possono essere, ad esempio, obblighi di riservatezza o di segretezza: riservatezza "proviene dal verbo latino *reservare re* - particella intensiva di -*servare*, che sta per mantenere, conservare, custodire, mettere da parte che, durante il Medio Evo, fu largamente usato nella terminologia giuridica"; segretezza ha un significato simile, dal latino *secretum* che è participio passato di *secernere*, ossia separare, mettere da parte, riporre. L'etimologia di privato, riservato e segreto, dunque, rimanda sempre a una separazione, ad una divisione: qualcosa è (o è reso) inaccessibile ad altri. La distinzione risiede nel fatto che il termine privato, in senso tecnico giuridico, si riferisce immediatamente alla "vita privata, personale e familiare, di una persona, di cui va tutelata e rispettata la riservatezza", dove la parola riservatezza designa proprio la caratteristica, in senso oggettivo, di inaccessibilità di determinati aspetti – dati, notizie - della vita di una persona[22].

La sfera privata dell'individuo è quell'insieme di fatti, comportamenti, scelte di cui deve essere garantita la riservatezza e che pertanto deve rimanere segreta, ossia inaccessibile a terzi e che si collega ad una sfera intima e familiare dell'individuo. La proiezione giuridica di tale sfera è la pretesa che essa rimanga inviolata: abbiamo definito tale pretesa diritto alla riservatezza per distinguerlo e contrapporlo alla *data protection*.

---

[22] Le etimologie di "riservatezza" e "segretezza" sono entrambe tratte dal *Grande Dizionario Italiano dell'Uso*, di Tullio De Mauro (Torino, UTET, 1999-2000).

Questa separazione tra fatto pubblico e privato, e quindi tra fatto accessibile e di pertinenza della collettività e dello Stato e fatto che non lo è, ha un'origine antichissima. Nell'antica Grecia[23] vi era una demarcazione chiara tra l'insieme di questi fatti, ossia la vita pubblica (*demion*), e la vita privata (*idion*); appartenevano alla vita pubblica, a titolo esemplificativo: la guerra, il bottino di guerra, il matrimonio, il processo. La collettività e lo Stato, chiaramente sovraordinati all'individuo, riconoscevano tuttavia l'esistenza di fatti privati che si svolgevano in determinati ambiti classicamente sottratti alla dimensione pubblica: la famiglia, la casa, il patrimonio. Si trattava di una distinzione ben radicata che è ancora oggi essenziale per comprendere la tutela della *privacy as intimacy* o *hard privacy*. Nel citare il patrimonio del re si indicava qualcosa che ricadeva in un contesto privato e non anche in una dimensione pubblica: si trattava di qualcosa che non riguardava la collettività.

Un'ulteriore conferma di quanto stiamo sostenendo si rinviene nel primo uso della parola privacy in ambito letterario: nel Troilo e Cressida, classico shakespeariano sulla guerra di Troia scritto nel 1602, si narra di come Achille si sottragga alla guerra, fatto pubblico per eccellenza perché riguardante la sopravvivenza stessa della collettività e dello Stato. Quando Ulisse si reca in ambasciata per convincerlo a tornare, Achille replica che ha buone ragioni per difendere la sua privacy, vale a dire la sua scelta di ritirarsi dalla dimensione pubblica:

---

[23] Hannah Arendt, cit., p. 19; Eva Cantarella, *Itaca – Eroi, donne, potere tra vendetta e diritto*, Milano, 2008, p. 90; Stefano Ferrucci, *L'oikos nelle leggi della polis. Il privato ateniese tra diritto e società*, in *Etica & Politica*, 2007, p. 135 e ss. Così anche nell'antica Roma: Wolfgang Sofsky, cit., p. 30.

"Ulysses: The cry went once on thee, And still it might, and yet it may again, If thou wouldst not entomb thyself alive And case thy reputation in thy tent; Whose glorious deeds, but in these fields of late, Made emulous missions 'mongst the gods themselves And drave great Mars to faction.

Achilles: Of this my privacy I have strong reasons.

Ulysses: But against your privacy The reasons are more potent and heroical: 'Tis known, Achilles, that you are in love With one of Priam's daughters"[24].

Quella che risulta a questo punto dell'*excursus* storico-letterario è una distinzione chiara perchè socialmente accettata tra due diversi contesti: uno pubblico riguardante la collettività e lo Stato ed uno privato riguardante l'individuo, distinzione che è già data e non tiene conto della (ed è indipendente dalla) volontà del soggetto. Pubblico e privato quindi perimetrano due contesti già dati e stanno ad indicare un particolare statuto sociale e giuridico di accessibilità o inaccessibilità dei fatti e delle informazioni che a quei contesti pertengono.

Accanto a questi due ambiti già delineati, possiamo però aggiungere ulteriori norme sociali e giuridiche che impongono regimi di accessibilità o inaccessibilità di dati

---

[24] Ulisse: …Un tempo il loro applauso era per te, e così potrebb'essere di nuovo, se rinunciassi a star sepolto vivo e a tenere racchiusa in una tenda la tua fama; tu, le cui grandi gesta su questi campi hanno indotto gli dèi a creare perfino in mezzo a loro frazioni avverse e tra loro in conflitto, e a trascinare a prendere partito perfino il grande Marte.
Achille: Il mio ritiro ha solide ragioni.
Ulisse: Ma ragioni più forti e più marziali s'ergono contro la tua secessione. Tutti sanno che sei innamorato di una delle figlie del re Priamo.

e/o informazioni. Possiamo allora aggiungere una terza ed una quarta categoria legata alla qualità di un'informazione o alla qualità del rapporto che lega due soggetti.

Nel primo caso, indipendentemente dal concetto di pubblico e privato (e quindi da un contesto pubblico o privato), l'informazione non è - e non deve essere - resa accessibile a terzi: tale informazione sarà riservata o segreta, indicando giustappunto il suo particolare statuto di inaccessibilità (o di limitata accessibilità) al di fuori dell'area entro cui deve e può legittimanente circolare; si pensi, a titolo di esempio, agli obblighi di riservatezza o ai segreti d'ufficio. La qualità del dato impone a uno o più soggetti di non renderlo accessibile al di fuori di coloro che sono autorizzati a conoscerlo ed utilizzarlo[25].

Nel secondo caso, avremo un diverso statuto di inaccessibilità che tiene in considerazione la qualità del rapporto che lega due soggetti e che pertanto impone degli obblighi, su uno dei due o su entrambi, di mantenere determinate informazioni o certi fatti riservati. Si pensi al rapporto tra cliente e avvocato. In questo caso facciamo riferimento all'istituto della confidenzialità[26]. Uno dei

[25] Lisa Austin, cit., p. 133.

[26] Nel Privacy Act statunitense del 1974 si faceva riferimento alle misure per garantire la sicurezza e la confidenzialità delle informazioni - Daniel J. Solove, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review*, 2006, p. 517; vedi anche Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, in *Stanford Law Review*, 2000, p. 1057; Alan E. Garfieldt, *Promises of Silence: Contract Law and Freedom of Speech*, in *Cornell Law Review*, 1998, p. 272 e ss.; Neil M. Richards, *The limits of tort privacy*, cit., p. 384; Geoffrey C. Hazard e Angelo Dondi, *Etiche della professionale legale*, Bologna, 2005, p. 279 e ss.

punti principali della nostra tesi è che la *data protection* potrebbe essere ricondotta ad analoghi obblighi di fedeltà di un soggetto (il gestore di una banca dati) nei confronti di un altro soggetto (l'interessato).

E' bene precisare che, in questi due casi (qualità del dato e qualità della relazione) possono essere vari: il segreto industriale tutela gli interessi economici di colui che svolge attività di impresa.

Rispetto a un dato, quindi, avremo o uno statuto di generale accessibilità oppure uno statuto di limitatata accessibilità in considerazione del (1) contesto privato al quale si riferisce, (2) della sua particolare qualità, (3) del particolare rapporto che lega due soggetti. Ci concentreremo solo sul primo punto.

Ritenere che il carattere pubblico o privato sia già dato non vuol dire affermare che lo statuto di accessibilità segua in modo automatico. Lo statuto di accessibilità (limitata o meno) dipende da valori diversi e origina diversi regimi giuridici. Si prendano ad esempio le nozioni di trasparenza amministrativa e di segreto di Stato. La trasparenza amministrativa consiste, nella sua accezione più ampia, nell'assicurare la massima circolazione possibile delle informazioni, contenenti o meno dati personali, all'interno dell'apparato statuale e all'esterno di esso. L'attività amministrativa dovrebbe perseguire criteri di pubblicità e di trasparenza (art. 1 legge 241/1990). Il principio di trasparenza qui è inteso come accessibilità alla documentazione dell'amministrazione o ai riferimenti da quest'ultima utilizzati nell'assumere una certa decisione: ciò dovrebbe implicare uno statuto di massima accessibilità. Per converso, la nozione di segreto di Stato implica che vi siano talune informazioni riguardanti pur sempre l'apparato amministrativo che non possono circolare nemmeno ai fini dell'accertamento di una

responsabilità penale. Si tratta di informazioni attinenti la segretezza militare per finalità di difesa da aggressioni esterne; il segreto politico interno a difesa delle istituzioni dello Stato democratico e degli organi costituzionali; infine il segreto politico dei rapporti internazionali non prettamente militari che riguardano le relazioni con gli altri stati. Ciò che chiarisce il modello di tutela è il valore che quell'insieme di regole mira a tutelare. Se tale valore è sfocato, anche il modello di tutela rischia di essere poco chiaro e dunque scarsamente efficace (o decisamente conflittuale).

Tornando alla distinzione tra privato e pubblico, dobbiamo riprendere i due significati di pubblico statuale e pubblico collettivo: se la sfera privata di una persona è un insieme di fatti non accessibili a terzi, la tutela di questa sfera privata potrà essere "verticale" (perché legata al rapporto di sovraordinazione dello Stato - pubblico statuale - sull'individuo o viceversa) oppure "orizzontale" (legata alla dialettica tra individuo privato e dimensione pubblica collettiva).

La sfera privata è quella dimensione dell'individuo inaccessibile a terzi in cui si esprime liberamente la possibilità di fare scelte e tenere comportamenti, dimensione delimitata dalla sfera pubblica in senso sia statuale sia collettivo, ossia, da un lato, dalla sfera di azione dello Stato in senso verticale e dall'altro dall'ingerenza della collettività in senso orizzontale.

Nella storia del diritto alla privacy questa distinzione ha senso per i particolari modelli di tutela che vi si collegano: la *constitutional privacy*, da un lato, e, almeno per quanto riguarda la tradizione statunitense, la *tort privacy*, dall'altro. Nell'uno e nell'altro caso, comunque, si tratta dell'emersione di un diritto tipicamente moderno perché legato indissolubilmente ad un rovesciamento del

rapporto di sovraordinazione tra individuo, da un lato, e pressione della collettività e dello Stato, dall'altro. In particolare la tradizione liberale rovescia il rapporto pubblico-privato: Benjamin Costant[27] la rappresenta perfettamente quando descrive la libertà (pubblica) degli antichi come contrapposta alla libertà (privata) dei moderni; da un lato l'autonomia politica collettiva quale massima espressione della libertà dell'individuo, dall'altro la libertà privata quale pacifico godimento dell'indipendenza del singolo. Ulteriore espressione di questo rovesciamento concettuale è il pensiero di Adam Smith nel momento in cui fa dipendere la ricchezza delle nazioni, quindi la ricchezza pubblica, dall'intraprendenza del privato. Mai prima di allora il perimetro della privatezza era stato tanto esaltato ed enfatizzato, mai prima di allora l'individuo era stato addirittura sovraordinato - almeno nella riflessione dei filosofi liberali - alla collettività e allo Stato, Stato che, in quest'ottica, avrebbe dovuto avere l'unica funzione di consentire agli individui quel pacifico godimento dell'indipendenza privata al quale ci siamo riferiti sopra. Ciò spiega, almeno in parte, l'emersione del valore della privacy in senso negativo e degli strumenti giuridici di tutela.

Ma non basta; il triangolo (i) individuo (privato), (ii) Stato e (iii) collettività (dimensioni del pubblico) registra, sempre in epoca moderna, un altro fondamentale protagonista: lo Stato nazionale[28].

A partire dal diciassettesimo secolo con

[27] Isaiah Berlin, cit., p. 289 e ss.

[28] Morton J. Horwitz, *The History of the Public/Private Distinction*, University of Pennsylvania Law Review, Vol. 130, No. 6 (Jun., 1982), pp. 1423-1428; Ugo Mattei, *Beni comuni. Un manifesto*, Bari, 2011, p. 35 e ss.

l'affermazione dell'assolutismo nella maggior parte degli Stati europei, s'inaugura un nuovo ordine internazionale, in cui il potere pubblico diventa eclusivamente potere statuale, oscurando il concetto di pubblico collettivo. L'interesse pubblico (statuale) si dilata oltre ogni limite ed in maniera prepotente: matura l'equivalenza tra Stato e diritto, insieme a quella tra diritto e realtà, che culminerà nelle grandi codificazioni napoleoniche in cui il sistema delle fonti del diritto mostra in modo evidente la riduzione pressochè totale del diritto alla legge (nazionale). Legge che pretende di normare tutta la realtà e non ammette lacune, comportando quella che è stata definita come saturazione normativa della realtà[29]. Ecco che in epoca moderna si stagliano quali protagonisti della speculazione filosofica e politica l'individuo privato e lo Stato nazionale.

Ciò che declina, quindi, è lo spazio comune, il pubblico inteso come collettivo, stretto tra l'esaltazione dell'individuo della tradizione liberale e la potenza dello Stato assoluto: sia sufficiente considerare quale esempio che nelle codificazioni ottocentesche si afferma solennemente che i beni sono o pubblici (statuali) o privati, *tertium non datur*.

La sintesi di queste tendenze contrapposte sul ruolo dello Stato e su quello dell'individuo privato si rinviene, ad esempio, nello sviluppo della teoria dei diritti umani, in cui la privacy intimità si inscrive perfettamente. Proprio nel periodo storico in cui la realtà equivale al diritto ed il diritto equivale allo Stato, la tradizione liberale cerca di delimitare l'ingerenza dello Stato nella vita

[29] Stefano Rodotà, cit., p. 9.

dell'individuo[30]. Come avremo modo di vedere, ciò avviene essenzialmente attraverso il riconoscimento di determinate garanzie.

3. La privacy quale libertà negativa

Se consideriamo la privacy quale bene giuridico, constatiamo che gli strumenti di tutela di tale bene sono diversi e possono essere ricostruiti a partire dai valori diversi che tutelano. Abbiamo individuato, infatti, almeno due categorie di valori fondamentali: la privacy in senso negativo (intimità o *hard privacy*) e la privacy in senso positivo (identità o *soft privacy*).

Concentriamoci sul primo valore della privacy prima accennato: il valore della privacy come libertà negativa.

La libertà negativa può essere definita come lo spazio di non interferenza del potere – essenzialmente statuale – rispetto alle azioni individuali: l'individuo gode di maggiore libertà laddove il potere non può ingerirsi nelle sue scelte, non può vincolarne le decisioni e non può ostacolarne i comportamenti. Il contenuto di tale libertà (e del relativo diritto) è un perimetro entro cui l'individuo può agire al riparo da invasioni esterne; definiamo tale perimetro sfera privata. Questa libertà dal controllo è il primo valore della privacy: attribuiamo valore alla privacy perché tale concetto esprime immediatamente una sfera di libertà di scelte e di comportamenti.

Si pensi ad esempio al tema della sorveglianza pubblica: dalla moltiplicazione delle telecamere di videosorveglianza ai nuovi dispositivi d'intercettazione informatica. Il corpo umano, come qualsiasi oggetto in

[30] John Rawls, cit., p. 15.

movimento, diviene controllabile a distanza con tecnologie satellitari o utilizzando le radiofrequenze, il che evoca gli studi di Michel Foucault sul carcere e il suo ruolo nella nascita delle moderne tecnologie di disciplina sociale. Il *panopticon* di Bentham diviene la metafora di una specie diversa e più completa di sorveglianza che si basa sui concetti di classificazione, normalizzazione ed esclusione[31]. La trasparenza determinata dalla visibilità e dalla registrabilità delle azioni individuali consente di perseguire esigenze statuali e collettive. Il bene giuridico sottostante a queste pratiche è generalemente collegabile alla sicurezza. Il controllo pubblico dovrebbe garantire la sicurezza di tutti. E' un luogo comune affermare che tali pratiche mettono a rischio la privacy, intesa quindi come rispetto di una sfera caratterizzata dall'accessibilità limitata a certi dati da parte di terzi (privata). Abbiamo quindi un interesse a celare certe informazioni o certi comportamenti e un contrapposto interesse a svelare. Il tema fondamentale è un tema di libertà ed il bilanciamento è tra un interesse privato (a celare) ed un interesse pubblico (a svelare). Come già anticipato, questi valori in conflitto consentono di meglio delineare i diritti e gli obblighi in materia.

Sul tema della trasparenza possiamo cogliere anche la differenza tra privacy in senso negativo e privacy in senso positivo: nel primo caso, come abbiamo visto, strumenti di controllo (e quindi di trasparenza) mettono in pericolo la privacy che è proprio la pretesa di non essere trasparenti per essere liberi di comportarsi come meglio si crede; nel secondo caso, come avremo modo di chiarire,

[31] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 9.

all'interno di una cornice relazionale tra chi raccoglie i dati e chi li cede, uno dei principi fondamentali è quello di trasparenza del gestore della banca dati nei confronti dell'interessato. Chi raccoglie i miei dati personali lo deve fare in maniera leale e corretta, perimetrando le operazioni che legittimamente potrà compiere su quei dati. Mi dovrà informare e dovrà consentirmi di accedere alle informazioni che mi riguardano presenti nella sua banca dati. Dovrà essere trasparente al fine di garantire la mia autodeterminazione informativa, vale a dire la mia identità in quel particolare perimetro in cui avviene il trasferimento di informazioni (ossia in quel particolare contesto – per questo parliamo di identità contestuale). Nel momento in cui il suo trattamento fuoriuscirà da quel perimetro avremo un trattamento illecito di dati. A nostro modo di vedere, qui non si tratta di una questione di libertà in senso negativo, quanto piuttosto di una questione di controllo dei nostri dati e di identità decontestualizzata. Si pensi al rapporto tra un cliente e la sua banca. L'istituto di credito deve essere trasparente nella raccolta delle informazioni sul suo cliente: sarà perfettamente ammissibile richiedere tutte le informazioni del caso riguardanti l'identità finanziaria del cliente: la sua propensione al rischio, le sue aspettative in termini di rendimento e gli impieghi futuri dei suoi risparmi. La banca dovrà usare queste informazioni all'interno della cornice relazionale (che chiameremo confidenzialità in riferimento al modello di tutela che riteniamo applicabile) delineata dalle norme sociali e giuridiche al riguardo. La banca potrà utilizzare queste informazioni entro tale perimetro.

Pertanto, la trasparenza in questo caso è uno strumento a tutela della privacy. Di un concetto di privacy, tuttavia, diverso da quello che stiamo descrivendo.

Infatti, un tema di libertà e di sorveglianza verrà

posto quando lo Stato introdurrà una legge per accedere a quelle informazioni per finalità, ad esempio, di accertamento e riscossione dei tributi. La trasparenza del *data holder* (la banca) nei confronti del *data subject* (il proprio cliente) diviene la trasparenza di quest'ultimo nei confronti dello Stato. Abbiamo due relazioni (cliente-banca e banca-Stato) che, come vedremo, sono rette da modelli di tutela dell'individuo diversi tra di loro.

Quale particolare manifestazione del più ampio concetto di libertà, nello scorso capitolo abbiamo considerato i diritti umani quali la prima declinazione giuridica della privacy-intimità: in questo senso il diritto alla privacy rientra nel novero ristretto dei diritti umani fondamentali, ossia di quei principi giuridici essenziali che sono evoluzione della plurisecolare tradizione dei diritti naturali, affacciatisi nella storia del diritto a partire dal diciottesimo secolo. Da ciò deriva, nella maggior parte dei casi, un insieme di principi sia a livello di trattati internazionali sui diritti umani sia a livello di carte costituzionali, insieme di principi in cui si manifesta l'esigenza d'ogni uomo di non essere arbitrariamente controllato o sorvegliato.

Come anticipato si tratta chiaramente di una forma di libertà tutt'altro che assoluta. Si potrebbe affermare che il problema centrale è quello di avere la massima privacy possibile – e, dunque, la massima libertà possibile rispetto a interferenze esterne – compatibilmente con gli altri interessi meritevoli di tutela.

Libertà del privato nei confronti della collettività e nei confronti dello Stato. Possibilità di agire senza condizionamenti e senza intrusioni.

Potremmo chiamarla "la libertà opaca"[32] perché, se riconosciuta dall'ordinamento, esprime la possibilità di sottrarsi dallo scrutinio dell'opinione pubblica (privacy orizzontale: in relazione a tale fenomeno nasce il primo modello di tutela moderno della privacy, la cosiddetta *tort privacy* di Warren e Brandeis[33] di cui parleremo oltre) e dei poteri costituiti (privacy verticale: nucleo essenziale del modello di tutela di quella che abbiamo chiamato *constitutional privacy*)[34].

Abbiamo parlato di altri interessi contrapposti al valore della libertà negativa in cui si sostanzia questa accezione di privacy. Oltre alla sorveglianza, un'altra pratica che si scontra con le esigenze della privacy è quella della pubblicazione attraverso mezzi di comunicazione di fatti riservati. L'origine stessa del "Right to privacy" in senso moderno risale al famoso articolo pubblicato da Warren e Brandeis e precedentemente citato, in cui si argomentava l'esigenza del riconoscimento di un illecito contro la stampa per la comunicazione di fatti veri – il che distingue il nostro tema da quello contiguo della

---

[32] Il diritto alla riservatezza diviene quindi uno strumento di "opacità" mentre la data protection, che tutela la privacy quale valore in senso positivo, è uno strumento di "trasparenza": Norberto Nuno Gomes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and articulating Rights*, in AA.VV, *Privacy and identity management for life*, Springer, 2010, p. 91; vedi anche Stefano Rodotà, cit., p. 103; Daniel Solove, *No privacy*, cit., p. 66 e ss.; Julie E. Cohen, *Privacy, Visibility, and Exposure*, in *Univeristy Chicago Law Review*, 2008.

[33] Samuel Warren e Louis Brandeis, *The right to privacy*, in *Harvard Law Review*, 1890, p. 193.

[34] Daniel Solove, *No privacy*, cit., p. 135 e ss.; Eugene Volokh, cit., p. 1108.

diffamazione[35] – ma privati: Warren e Brandeis sostenevano che la *common law* dovesse porre rimedio al pregiudizio emotivo che subiva chi si trovava involontariamente al centro delle attenzioni della stampa per fatti privati non connotati da rilevanza pubblica. La tensione tra la privacy e la "freedom of expression" è eclatante: la libertà individuale intesa come libertà da interferenze esterne avrebbe dovuto quindi limitare un altro principio sacro della tradizione liberale, ossia la libertà di espressione. Non molto è cambiato: il concetto di privacy come valore che si sostanzia nella libertà negativa ostacola una serie di attività di grande rilievo. La "libertà opaca", anzitutto, confligge chiaramente con la manifestazione del pensiero nella sua forma di diritto d'informare e d'informarsi; pone dei vincoli alla diffusione d'informazioni volte a tutelare l'interesse alla trasparenza e al buon andamento della pubblica amministrazione, alla captazione di informazioni nell'ambito delle attività di indagine per l'accertamento e la repressione dei reati, alla raccolta di informazioni per esigenze di sicurezza nazionale, alla profilazione della clientela per finalità di *business intelligence*. È altrettanto chiaro che, essendo queste attività espressione di altri valori parimente tutelati a livello normativo, il concetto di privacy come principio giuridico (per citare "L'etica dei principi" di Zagrebelsky[36]) deve essere quindi bilanciato con tutti i suddetti interessi, riconosciuti espressamente dall'ordinamento. Vedremo che il modello di tutela che ne segue, sia in termini di *tort privacy* sia in termini di

[35]Neil M. Richards, *The limits of tort privacy*, cit., p. 363.
[36]Gustavo Zagrebelsky, *Intorno alla legge. Il diritto come dimensione del vivere comune*, Torino, 2009, p. 28.

constitutional privacy, pone un perimetro privato (vita privata, famiglia, domicilio, comunicazioni) e un perimetro pubblico (collettivo o statuale). Il primo è caratterizzato da uno statuto di limitata accessibilità o disponibilità di fatti, comportamenti, informazioni; quando detto statuto viene messo in discussione, prevale la libertà negativa salvo che non sussista un chiaro interesse pubblico prevalente.

Molto spesso questo perimetro privato ha dei confini fisici (ad esempio la propria abitazione) e in tal senso è possibile parlare di "*spatial privacy*"[37]. In realtà ciò che rileva è una ragionevole aspettativa che alcune informazioni o certi comportamenti siano limitatamente accessibili ai terzi.

Allo stesso modo e specularmente, il perimetro collettivo e statuale dovrebbe caratterizzarsi per la trasparenza dei fatti, dei comportamenti e delle informazioni.

A conclusione della riflessione fin qui svolta, vale fissare un punto di grande importanza: la proiezione giuridica della privacy, vista come libertà negativa, si sostanzia in una serie di garanzie, di solito fissate a livello costituzionale (contro l'ingerenza statuale) e penale (contro l'ingerenza di altri membri della collettività), ammettendo deroghe solo a condizione della sussistenza di un prevalente interesse pubblico e nel rispetto di determinate garanzie.

4. La privacy quale libertà positiva

La privacy quale libertà positiva, invece, ritaglia uno

[37] Neil M. Richards, *Intellectual privacy*, cit., p. 413.

spazio di autonomia nella costruzione della propria identità personale. Si afferma, in tal senso, una pretesa di controllo sulle informazioni personali che circolano nello spazio pubblico: per questa ragione si parla di *informational privacy*[38].

La sottrazione dalla sfera pubblica (il valore della privacy quale libertà d'azione in senso negativo) e le garanzie giuridiche correlate (diritto alla privacy anch'esso colto in senso negativo) si trasformano in autonomia (o autodeterminazione) informativa.

Si passa dalla libertà dall'essere controllato, alla libertà di controllare le proprie informazioni.

Deve essere il singolo a decidere in autonomia sulla cessione e sull'utilizzo dei dati che lo riguardano tanto più nel momento in cui si palesano rischi derivanti dal trattamento di enormi quantità dei dati per mezzo di sistemi informatici. Non si tratta semplicemente di sottrarsi dall'identificazione (altrimenti sarebbe stata un'esigenza

---

[38] Per una definizione vedi Luciano Floridi, *The ontological interpretation of informational privacy,* Springer, 2006. Per l'A., l'*informational privacy* "*is a function of the onthological friction in the infosphere. Many factors can affect the latter, including, most importantly, technological innovations and social developments. Old ICTs affected the ontological friction in the infosphere mainly by enhancing or augmenting the agents embedded into it; therefore, they tended to decrease the degree of informational privacy possible within the infosphere. On the contrary, digital ICTs affect the ontological friction in the infosphere most significantly by re-ontologizing it; therefore, not only can they both decrease and protect informational privacy but, most importantly, they can also alter its nature and hence our understanding and appreciation of it"*.

meramente negativa) ma di condividerli in maniera consapevole (*data sharing*). Nell'epoca delle banche dati e di Internet, ossia di un iper *data base*, vi può essere un maggiore interesse per il singolo nel controllare le informazioni che circolano su di sé piuttosto che impedire ingerenze dall'esterno, soprattutto nel momento in cui la quantità delle informazioni in rete, e quindi facilmente accessibili, aumenta in maniera vertiginosa. La dicotomia privato - pubblico, così come quella accessibile - inaccessibile che ne è il cuore, resta importante ma gradatamente sfuma e perde centralità. Il nuovo *focus* è l'insieme di informazioni personali che costituiscono la nostra identità e i requisiti del trattamento di queste informazioni da parte dei soggetti che detengono banche dati[39]. Abbiamo quindi una relazione: da una parte il soggetto cui quei dati si riferiscono e che vuole che la sua identità sia tutelata e, dall'altra parte, il gestore della banca dati che vuole raccogliere, utilizzare e comunicare questi dati. Proprio perché ci troviamo in una cornice di relazione, l'autodeterminazione riguardo alle informazioni personali - la privacy quale valore in senso positivo - si realizza in modo mediato, attraverso l'imposizione di condizioni di liceità del trattamento delle informazioni stesse. Il fuoco normativo si sposta dal diritto dell'interessato all'obbligo di colui che tratta i dati. Il valore da tutelare è la possibilità dell'interessato di decidere in ordine alla sua identità all'interno di un contesto di relazione.

La privacy quale valore negativo è il perimetro entro

[39] Daniel J. Solove e Chris Jay Hoofnagel, *A Model Regime Of Privacy Protection*, in *University of Illinois Law Review*, 2006, p. 363.

cui le nostre scelte e i nostri comportamenti non sono sottoposti all'altrui controllo perché legati a certi contesti privati[40]; la privacy quale valore positivo è il controllo che l'individuo può esercitare nella sfera pubblica riguardo modalità e tempi di raccolta e di circolazione delle informazioni che lo riguardano. Nel primo caso abbiamo contesti tradizionalmente già delineati; nel secondo caso contesti particolari da delineare attraverso regole di relazione. Nel primo caso uno statuto di limitata accessibilità delle informazioni legato a questi contesti dati; nel secondo caso un medesimo statuto dipendente da una relazione (e magari dalle sue asimmetrie). Nel primo caso la domanda fondamentale è qual è il grado di controllo che gli altri (lo Stato e la collettività) possono esercitare nei confronti dell'individuo quando questi si muove in contesti privati; nel secondo caso la domanda fondamentale è qual è il grado di controllo che l'individuo può esercitare nei confronti dei propri dati personali quando entra in relazione con i gestori delle banche dati. Le due domande danno luogo a due risposte necessariamente distinte ed eterogenee. Nel primo caso, vi sono essenzialmente garanzie costituzionali e norme penali e civili a tutela di questi spazi di libertà (quindi consideriamo un diritto tipicamente individuale); nel secondo caso, vi sono obblighi in capo al *data holder* e correlativamente diritti attribuiti al *data subject* (quindi consideriamo un diritto tipicamente relazionale).

Facciamo un esempio di temi che coinvolgono la prima domanda: qual è il controllo che il pubblico esercita

[40] Wolfgang Sofsky, *In difesa del privato*, cit., p. 87; Daniel J. Solove, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review*, 2006, p. 549 e ss.

sul privato? In tempi recenti, un esempio ben noto è rappresentato dalla politica statunitense dopo i tragici fatti dell'11 settembre 2001. Il potenziale conflitto tra "privacy e sicurezza"[41] ha visto prevalere quest'ultima diminuendo le garanzie individuali. L'interesse generale alla prevenzione del terrorismo è senza dubbio importante, come è importante la libertà dell'individuo di non subire interferenze ingiustificate nella propria vita privata. Come avremo modo di chiarire, la tradizione giuridica occidentale ha sempre ritenuto prevalente l'interesse privato salva la presenza di un interesse pubblico chiaramente individuato da una legge e declinato attraverso una serie di garanzie volte a prevenire gli abusi del potere pubblico[42].

Facciamo quindi un esempio di temi che coinvolgono la seconda domanda. Che uso può essere fatto da un Internet Service Provider che gestisce un motore di ricerca dei dati dei suoi utenti? Se il risultato di una particolare ricerca viene ritenuto pregiudizievole, posso chiedere la rimozione di questi dati. Ho il controllo della mia identità? Perché chiaramente il controllo che l'individuo può esercitare sui suoi dati personali nello spazio pubblico plasma la sua identità ed il valore della privacy in positivo si sostanzia nel dare la possibilità all'individuo di decidere come condividere i propri dati. Il dominio sul corpo fisico diviene dominio sul corpo elettronico. In questo senso il valore della privacy in senso positivo (*privacy as identity*) dà forma alla regolamentazione sulla *data protection*. Ma è un dominio possibile? Esaminiamone la regola fondamentale: ogni individuo può pretendere che l'uso dei

[41] Helen Nissenbaum, cit., p. 114.
[42] Neil M. Richards, *Intellectual privacy*, cit., p. 433.

suoi dati personali si svolga nel rispetto dei suoi diritti e delle sue libertà fondamentali, nonché della sua dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Ciò che maggiormente rileva, tuttavia, è che questa pretesa deve essere esercitata dal soggetto cui si riferiscono i dati (*data subject*) direttamente nei confronti del gestore della banca dati (*data holder*). Chi gestisce i dati deve farlo per finalità compatibili con dignità, riservatezza e identità personale dell'interessato.

L'aspetto più importante dunque si rinviene nella considerazione del rapporto tra due soggetti - il *data holder* ed il *data subject* – si tratta quindi di un controllo mediato.

Emergono, in questo contesto, differenze teoriche di grande importanza che abbiamo già anticipato: anzitutto, parliamo di dati personali e non di dati privati. Quindi di identità all'interno di un contesto di relazione e non di riservatezza della vita privata; di trasparenza nella relazione tra *data subject* e *data holder* e non di opacità sulle scelte e sui comportamenti dell'individuo. Abbiamo visto che i dati personali sono le informazioni relative a un soggetto identificato o identificabile, anche indirettamente, mediante il riferimento a qualsiasi altro dato. L'ambito d'applicazione della normativa non sono i fatti che si svolgono nella sfera privata dell'individuo perché il valore di riferimento non è la privacy quale particolare forma di libertà negativa, bensì i dati personali che costituiscono la nostra identità. Si passa da un significato forte di privatezza, tradizionalmente legato a determinati contesti (la casa, la famiglia, le comunicazioni) particolarmente meritevoli di tutela contro le ingerenze esterne ad uno più sfumato coincidente con un particolare statuto di limitata accessibilità ed utilizzabilità delle informazioni personali

condivise e memorizzate in una banca dati. Da una libertà di agire al riparo da invasioni da parte di terzi si passa a una libertà di determinare la propria identità, di incidere sulla circolazione dei dati che ci riguardano.

In secondo luogo non parliamo tanto del diritto (e delle garanzie) di cui l'individuo cui quei dati pertengono (*data subject*) gode nella propria dimensione privata, quanto piuttosto degli obblighi di chi vuole trattare i dati personali (*data holder*) nell'ambito di un'attività professionale, o comunque non privata (è noto, infatti, che la normativa sulla *data protection* si applica solo a trattamenti che esulano da finalità meramente private, salvo i casi di comunicazione sistematica o diffusione dei dati). La possibilità di decidere sulla propria identità passa attraverso l'imposizione di obblighi sul detentore della banca dati: il *data holder* deve garantire la riservatezza delle informazioni personali, ossia l'inaccessibilità a terzi non legittimati rispetto ai dati che il *data subject* condivide con lui.

In sintesi: non è più questione di perimetri privati e pubblici già dati ma di un perimetro relazionale da tracciare tra *data holder* e *data subject*. E rispetto a un confine da disegnare in base alle varie possibili relazioni tra i due soggetti coinvolti, non sempre vi saranno norme sociali e giuridiche a guidarci[43]. L'esempio più eclatante è quello dei social network: oggi riteniamo normale condividere una grande quantità di informazioni personali di cui magari tra dieci anni potremo vergognarci. Oppure intratteniamo relazioni con perfetti sconosciuti ai quali comunichiamo informazioni che non confidiamo ad amici e conoscenti. E tutti questi dati sono memorizzati e

[43] Helen Nissenbaum, cit., p. 119 e ss.

utilizzati su server di società che si trovano dall'altra parte del mondo e sulle quali non ci è possibile esercitare alcun tipo di controllo.

Abbiamo già scritto che, rispetto a un dato, avremo uno statuto di generale accessibilità oppure uno statuto di limitatata accessibilità in considerazione: (1) del contesto privato al quale si riferisce, (2) della sua particolare qualità oppure (3) del particolare rapporto che lega due soggetti. Ebbene: riteniamo che sia la singola qualità del dato (il fatto che sia riferibile a una persona identificata od identificabile) e la particolare relazione che stringono i due soggetti (*data subject* e gestore della banca dati) a determinare un particolare statuto di accessibilità; non il contesto privato e pubblico di riferimento. Ad esempio: in un contesto medico non conta tanto che le informazioni siano pubbliche e private. Le norme giuridiche e sociali riguardanti la circolazione delle informazioni personali si basano sulla considerazione della relazione tra medico e paziente e sul tipo di informazione che viene condivisa. Sino a quando le informazioni sulla nostra salute circolano in contesto medico, non sussiste una violazione della nostra privacy (intesa quale valore positivo). La nostra identità di paziente, in questo caso, viene preservata. Ciò posto vi può essere una doppia violazione della privacy: da parte del medico che potrebbe comunicare questi dati fuori da tale contesto, ad esempio a società interessate a queste informazioni. Questo è un tema di *data protection*. Da qualsiasi altro soggetto interessato ad accedere a quelle informazioni (lo definiamo *stake holder*), ad esempio un giornalista, e in questo caso avremo un tema di diritto alla riservatezza.

La privacy come libertà positiva, ossia l'autodeterminazione informativa, riguarda, dunque, una sfera diversa da quella intima e personale di un soggetto,

ossia la sfera delle informazioni che vengono condivise con l'esterno, che circolano (o non circolano) nello spazio pubblico in base a quel particolare perimetro relazionale - il contesto entro cui avviene lo scambio informativo - che abbiamo richiamato.

Per questo parliamo di identità contestuale, che possiamo definire come l'insieme delle informazioni personali legate a un determinato contesto entro cui si svolge la relazione tra *data holder* e *data subject*. Va da sé che il concetto di identità richiama principalmente il concetto di persona, imponendone una definizione, ai fini che qui rilevano. Per i latini la "persona" (da *per-sonar*: risuonare) era la maschera di legno portata sulla scena dagli attori, caratterizzata da un'esasperazione dei tratti del viso, quasi caricaturali, e dall'apertura in prossimità della bocca realizzata in modo da potenziare il suono della voce (*ut personaret*). Il personaggio, quindi, era l'individuo rappresentato sulla scena e analogamente la persona è l'essere umano inserito in un ordine sociale che stabilisce ruoli e qualità, così come la persona in senso giuridico è l'individuo inserito in un ordine normativo in grado di fissare diritti e doveri. Così, le informazioni sulla persona, sull'individuo colto nel generale contesto sociale, rappresentano l'oggetto della disciplina sulla protezione dei dati personali sulla base del valore dell'autodeterminazione informativa che afferma che debba essere l'individuo stesso a scegliere le informazioni che vuole condividere. Queste informazioni costituiscono l'identità (fisica, personale, digitale) della persona, ciò che distingue un individuo dagli altri all'interno di una società.

Quello che riteniamo si debba evidenziare è la valenza contestuale del concetto di identità personale.

Sempre porgendo la massima attenzione alla questione definitoria, vale citare Pfitzemann[44], nonché la nota distinzione tra *idem* e *ipse* di Paul Ricoeur: l'identità è la prospettiva dell'osservatore che oggettiva il soggetto, rendendolo un insieme di attributi, così da consentire il confronto tra persone diverse (*idem*). La prospettiva del soggetto, invece, rappresenta il senso di sé in prima persona (*ipse*). Pertanto, grazie agli strumenti forniti da questi autori, è possibile affermare che l'identità personale è l'insieme di attributi sociali (*idem* o *me*) riferibili ad una persona.

La *data protection* tutela non tanto la riservatezza, ossia la possibilità di rendere inaccessibili determinate informazioni, quanto piuttosto l'identità di una persona in un contesto sociale, ossia la circolazione delle informazioni personali in attività professionali. O, per meglio dire, rappresenta un primo livello di tutela. Non vi è più un dominio privato e pubblico (statuale o collettivo); vi è la nostra identità personale in un certo contesto (ad esempio, le informazioni sulla nostra salute, la nostra identità di paziente). A questo riguardo, uno dei concetti più interessanti sviluppati da Pfitzemann è quello di identità parziale[45]. Egli parte dal presupposto che non tutti

---

[44] Andreas Pfitzmann e Marit Hansen, *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management"* reperibile http://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html, 2010, p. 29.

[45] Andreas Pfitzmann e Katrin Burcea-Pfitzmann, *Lifelong Privacy: Privacy and identity management for life,* Springer, 2010, p. 4; Marit Hansen, *Marrying Transaprency Tools with User-Controlled Identity Management,* in AA.VV, *IFIP International*

gli attributi (si pensi, ad esempio, a nome e cognome) restino legati alla persona in maniera definitiva. Al contrario, dato un certo contesto, gli attributi riferibili ad una persona sono tendenzialmente limitati ad esso. Il che vuol dire che, prendendo in considerazione molteplici contesti, a questi corrisponderanno molteplici identità; per questa ragione egli parla di identità parziali. Le violazioni della privacy in senso positivo sono violazioni della parzialità della nostra identità, ossia del fatto che le informazioni che possono circolare in un dato contesto vengono utilizzate fuori da esso. Il particolare contesto di riferimento determina le norme sociali e giuridiche che regolano lo scambio di informazioni considerato normale o ammissibile. Si pensi, ad esempio, a un contesto professionale in cui risulterà del tutto normale scambiare informazioni relative alle proprie esperienze lavorative, decisamente meno parlare di quelle riguardanti le proprie opinioni politiche. L'identità personale, quindi, è condizionata dal contesto in senso sincronico: ciò che è ammissibile se riferito ad un contesto, può non esserlo se decontestualizzato.

Occorre poi aggiungere che la violazione dell'identità contestuale può nascere anche dal fatto che la circolazione delle informazioni, ammissibile in un determinato momento, viene percepita come violativa della nostra privacy se effettuata a distanza di tempo. Infatti gli attributi di una persona sono anche destinati a mutare nel tempo. In concreto: le medesime informazioni mediche devono essere (ed è ragionevole che siano) costantemente aggiornate e la loro conservazione è

Federation for Information Processing; The Future of Identity in the Information Society, Springer, 2008, p. 201.

giustificata solo nell'ottica di una migliore comprensione dello stato di salute del paziente in quel particolare momento. Le informazioni su di una persona sono destinate in massima parte a evolvere, a modificarsi. In passato questa evoluzione portava spesso alla cancellazione e alla dimenticanza delle informazioni precedentemente acquisite. Oggi non è più così: un aspetto molto importante è che la registrazione di queste informazioni si accumula e rende la nostra identità un fenomeno incrementale[46]. L'identità personale è condizionata dal contesto, dunque, anche in un senso che potremmo definire diacronico[47].

La domanda fondamentale quindi è: qual è il grado di controllo che l'individuo può esercitare sui propri dati personali in senso sincronico, ossia impedendo che le informazioni vengano decontestualizzate, ed in senso diacronico, ossia impedendo che le informazioni persistano nel tempo?

A tale ultimo riguardo, particolare interesse desta il dibattito sul diritto all'oblio, ossia sulla tutela della pretesa di chi non vuole che i propri dati personali diventino patrimonio permanente del web o di altri mezzi di comunicazione e chiede di essere dimenticato dalla rete, rivendicando dunque una sorta di diritto all'oblio, del quale si tratterà più avanti. In quest'ottica, come sostiene Helen Nissenbaum[48], la privacy quale valore positivo può

---

[46] Andreas Pfitzmann e Katrin Burcea-Pfitzmann*, Lifelong Privacy: Privacy and identity management for life,* cit.*,* p. 13; John Palfrey e Urs Gasser, *Nati con la Rete*, Milano, 2009, p. 94 e ss.

[47] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 11.

[48] Helen Nissenbaum*, Privacy in Context,* in *Stanford University Press*, 2009, p. 120, 129.

ridursi alla tutela della propria identità contestuale, ossia alle specifiche regole di appropriatezza dei flussi di informazioni personali modellate sulle norme sociali e giuridiche di quel particolare contesto. Avremo *data subject* e *data holder*, tipo di informazione, vincoli dei flussi informativi (alcuni ammessi, altri non ammessi). In genere, quando il flusso d'informazione rispecchia norme sociali e giuridiche ben radicate, non vi sono problemi di sorta. Quando, tuttavia, queste norme ancora non ci sono, oppure quando ci sono e vengono violate, vi sarà un conflitto tra chi desidera la circolazione di quell'informazione e chi non la desidera. Restando fermi all'esempio medico, sono i pazienti stessi ad aspettarsi che i loro medici condividano queste informazioni con degli specialisti a seconda delle necessità. Si assisterebbe a una chiara violazione della privacy, invece, se i medici vendessero quelle stesse informazioni oppure le pubblicassero su Internet rendendole accessibili a chiunque. In relazione al contesto medico, dunque, ci sarebbe una chiara violazione del parametro dell'appropriatezza che dovrebbe essere il limite atto ad impedire il flusso informativo.

La tutela dell'autodeterminazione informativa passa per il rispetto di obblighi di confidenzialità entro un determinato contesto di relazione da parte di chi gestisce queste informazioni. La normativa sulla *data protection* dà forma a queste regole di appropriatezza utilizzando i principi fondamentali di necesarietà e finalità piuttosto che quello di contesto: posta la base legale del trattamento (sia essa una manifestazione di volontà o una disposizione di legge) il *data holder* può trattare tutti e solo quei dati necessari al conseguimento di una certa finalità. Potremmo dire che la normativa sulla *data protection* obbliga a delineare quei contesti a cui si riferisce la Nissenbaum;

tale obbligo però non è sufficiente a generare le norme sociali che consentono di definire un certo flusso informativo appropriato o meno.

Si pensi, ad esempio, alle tecnologie dell'informazione e ai media digitali, considerati costanti minacce alla privacy[49]. Nonostante gli obblighi di legge, non esistono ancora norme sociali di appropriatezza: non è possibile richiamare i concetti, sopra analizzati, di pubblico e privato e nemmeno ci si può accontentare degli obblighi legalmente imposti e largamente disattesi. Il fatto che le informazioni che si trovano in Internet siano facilmente e generalmente accessibili dovrebbe quanto meno farci riflettere. L'eventuale circolazione di un'informazione personale fuori dall'ambiente entro il quale può – e, in un certo senso, deve – circolare provocherebbe inevitabilmente una lesione della privacy, da leggersi in senso positivo, secondo i parametri sopra enunciati. Questa è quella che possiamo definire una violazione in senso sincronico. Vale precisare che parlando di contesto non ci si limita a considerare quello spaziale ma si estende il concetto anche a quello temporale; l'informazione personale, infatti, può essere fuori contesto anche perché particolarmente datata. Questa, a differenza della precedente, è una violazione in senso diacronico.

Definire quest'aspetto *soft privacy* può essere utile dal punto di vista della genesi del modello di tutela che poi andremo ad analizzare ma sicuramente occorre prendere atto che il valore che abbiamo di fronte e che rappresenta la sostanza della *data protection* è la tutela dell'identità

[49] Manuel Castells, *Galassia internet*, Milano, 2006, p. 165; Alessandro Acquisti, *Privacy,* in *Rivista di Politica Economica*, 2005, p. 328.

contestuale, come precedentemente definita, cui necessariamente rimanda il concetto stesso di autodeterminazione informativa. Si tratta di un primo livello di protezione legato alla relazione tra *data subject* e *data holder* e dipendente dal contesto in cui avviene il *data sharing*. Lo statuto di limitata accessibilità delle informazioni deriva dal tipo di informazione e dalla relazione piuttosto che dalla tutela di un determinato contesto che qualifichiamo come privato.

Il controllo sulle proprie informazioni personali è un valore che prescinde da quello di libertà dalle altrui interferenze e che si sostanzia nella tutela dell'identità contestuale - *privacy as contextual identity* -, tutela più o meno articolata a seconda delle norme sociali e giuridiche esistenti in relazione a quel determinato contesto. E' chiaro che una relazione medica (e quindi la nostra identità di pazienti) è normata sia dal punto di vista sociale che dal punto di vista giuridico e la *data protection* non aggiunge molto a quanto già noto. L'elemento da tenere in considerazione, piuttosto, è che la tradizione europea della *data protection* estende e generalizza un obbligo di confidenzialità molto stringente.

Ciò detto, diversi strumenti normativi possono concorrere a tutelare detto valore. La sua prima proiezione giuridica, ovvero il diritto all'identità personale, è definibile come la pretesa dell'individuo, nel momento in cui è identificato – e non agisce, quindi, anonimamente – di vedersi descritto esattamente per quello che egli è, senza inesattezze che possano distorcerne la personalità agli occhi del pubblico (della collettività). La *data protection* ne rappresenta una seconda proiezione giuridica, in cui emerge un concetto più specifico, quello appunto di identità contestuale, come l'abbiamo descritta sopra. Il perimetro di relazione tra *data holder* e *data subject* è il

contesto entro cui vengo scambiate le informazioni, lo spazio nel quale il *data holder* dovrà rispettare le norme sociali e giuridiche volte ad evitare la decontestualizzazione, sincronica o diacronica, di quelle informazioni. Un terzo istituto giuridico è quello della confidenzialità – che riteniamo largamente sovrapponibile con quello della *data protection*, in cui il confidente ha alcuni obblighi in relazione all'utilizzo delle informazioni che apprende. Siccome gli obblighi del confidente hanno contenuto simile a quelli del *data holder*, come avremo modo di chiarire successivamente, possiamo anche parlare della *data protection* come di una nuova forma di confidenzialità; di ciò scriveremo diffusamente più avanti.

Si delineano così sempre più nitidamente le aree delle quali qui ci si occupa: una triangolazione tra privacy (in senso negativo – *privacy as intimacy*), identità personale (*rectius* contestuale – *privacy as contextual identity*) e *data protection*; *data protection* ed identità sono in rapporto di mezzo a fine, mentre la *privacy as intimacy*, protetta solo indirettamente dalla disciplina della protezione dei dati personali, trova invece tutela immediata in quelle norme (costituzionali, penali e civili) che salvaguardano determinati contesti privati.

Pertanto, la tutela della sfera privata (privacy in senso negativo – *hard privacy* perché meglio definita ed articolata nella tradizione giuridica occidentale) è qualcosa di diverso dalla tutela dell'identità personale o autodeterminazione informativa (privacy in senso positivo – *soft privacy* perché più elastica ed adattabile ai mutevoli interessi delle parti in causa). E la *data protection*, come avremo modo di appurare, delinea un modello di tutela

procedurale[50] e non sostanziale in primo luogo del valore della *privacy as identity* e, in modo mediato e non essenziale, del valore *privacy as intimacy*. Il Global Privacy Standard è oggi la prima espressione sovranazionale di questo modello di tutela procedurale e volto alla protezione immediata dell'identità contestuale.

Infatti l'autonomia (o autodeterminazione) informativa - che attiene, dunque, alla privacy colta come valore in senso positivo - riguarda la nostra identità personale (*rectius* contestuale) più che la nostra privatezza: essa cesella la nostra identità all'interno della sfera pubblica. Il dato personale è il mattone della nostra identità, un elemento essenziale, fondante e imprescindibile. La privacy in senso positivo si circoscrive così come la parte di scelta lasciata all'interessato nella costruzione della propria identità. Tale possibilità di scelta, come anticipato, non è priva di limiti, e ciò anche per quanto concerne la propria origine: essa, infatti, è spesso funzione del potere esercitato da un soggetto nei confronti dell'altro. In questo senso può dirsi che la *data protection* mira a correggere asimmetrie di potere in relazione ad informazioni personali.

---

[50] Norberto Nuno Gomes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and articulating Rights*, cit., p. 97; Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, in *Michigan State University College of Law Journal of International Law*, 2007, p. 41 e ss.

CAPITOLO II – I MODELLI DI TUTELA DELLA PRIVACY

Come anticipato nella parte di trattazione già svolta, possiamo distinguere un valore della privacy in senso negativo (libertà dall'essere controllato – *hard privacy* o *privacy as intimacy*) e uno in senso positivo (libertà di controllare le proprie informazioni – *soft privacy* o *privacy as identity*); quest'ultimo valore attiene alla nostra autodeterminazione informativa ed in definitiva alla tutela della nostra identità rispetto a violazioni del contesto in cui lo scambio di informazioni è avvenuto (*privacy as contextual identity*).

Questo secondo capitolo, in particolare, si concentrerà principalmente – ma non esclusivamente – sulla tutela di questi valori.

La privacy in senso negativo porta con sé un modello di regolamentazione a tutela della sfera privata dell'individuo. Storicamente, il primo modello di tutela della privacy, nel 1890, fu il modello nordamericano del "*right to be let alone*": la pubblicazione di fatti privati era considerata una vera e propria minaccia all'intimità delle persone, fonte di danno e quindi azionabile davanti a un giudice: è la *tort privacy* di Warren e Brandeis che trae origine dall'estensione del modello proprietario (*privacy as property*) dalle cose ai sentimenti di tranquillità e intimità[51]. Nel 1928, Brandeis, diventato nel frattempo

[51] Richard A. Posner, *The Economics of Justice*, Harvard University Press, 1981, p. 231 e ss.

giudice della Corte Suprema, utilizzò il "diritto di essere lasciato in pace" per dissentire in un celebre caso (Olmstead *vs* United States) che riguardava la compatibilità tra le intercettazioni e il Quarto Emendamento. Secondo Brandeis la privacy avrebbe dovuto impedire ogni intrusione arbitaria da parte del governo nella vita privata delle persone, qualunque fosse il mezzo utilizzato. Anche nelle successive cause Griswold *vs* Connecticut e Roe *vs* Wade, la Corte si è basata sulla stessa idea per articolare la tutela costituzionale del diritto alla privacy. Prenderemo le mosse da questo modello di tutela (*privacy as dignity*) che, a nostro giudizio, influenza anche la soluzione delle controversie in materia di *tort privacy*.

A partire dagli anni '70, infine, dinnanzi al moltiplicarsi delle banche dati e dei trattamenti di dati personali muta il riferimento al valore della privacy in senso negativo ed emerge la libertà di controllare le informazioni che ci riguardano: è il *right to privacy* in senso moderno che dà origine alla disciplina sulla protezione dei dati personali e al Global Privacy Standard. Si impongono sul *data holder* una serie di obblighi procedurali volti a tutelare la riservatezza (inaccessibilità) delle informazioni archiviate ed utilizzate (*privacy as - new - confidentiality*). Infine, con la nascita della rete Internet, la possibilità di memorizzare, aggregare, analizzare, diffondere informazioni – personali e non – impone un nuovo modello di tutela quale evoluzione della confidenzialità posta a tutela dell'identità contestuale dell'individuo (*privacy as contextual identity*).

1. Privacy e sorveglianza: *privacy as dignity*

La protezione dei dati personali sottende la libertà

positiva (o di autodeterminazione informativa) del *data subject*; la tutela fornita a questo valore viene concepita essenzialmente come imposizione di obblighi sul *data holder*, tenuto al rispetto di norme ben precise in materia di trattamento e circolazione dei dati stessi. La protezione dei dati personali è solo uno degli strumenti usati per tutelare la privacy come valore positivo. Secondo la sua moderna interpretazione, quindi, il valore privacy finisce per coincidere con la libertà di autodeterminare la propria identità esercitando un controllo sui propri dati personali e sulla loro circolazione. Tuttavia, sarebbe errato limitare a ciò la privacy, poiché il diritto alla privacy ha un ambito d'applicazione decisamente più esteso.

Attribuiamo valore alla privacy in quanto a tale concetto si rcollega una sfera di libertà negativa: ossia la possibilità per l'individuo di agire al riparo da intromissioni esterne; l'abbiamo definita libertà dall'essere controllato[52]. Quanto abbiamo sin qui articolato, ossia una distinzione tra privacy (intimità) in senso negativo e privacy (identità) in senso positivo, trova conferma nella Carta dei diritti fondamentali dell'Unione Europea[53], dove troviamo due diversi articoli dedicati al tema: il primo sul diritto alla privacy come libertà negativa, il secondo sul diritto alla protezione dei dati personali (privacy come libertà positiva). Si fa riferimento, in particolare, all'articolo 7 e all'articolo 8, il primo dedicato a quella che

---

[52] Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 493; Daniel J. Solove, *Conceptualizing privacy*, cit., p. 1116; Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, in *Boston College Law Review*, 2007, p. 620 e 637.

[53] Stefano Rodotà, *Data protection as a fundamental right*, in AA.VV. *Reinventing data protection?*, Springer, 2009, p. 77 e ss.

abbiamo definito privacy intimità ed il secondo alla privacy identità. Infatti, l'articolo 7, rubricato "Rispetto della vita privata e della vita familiare", stabilisce che: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni". L'articolo 8, invece, reca la rubrica "Protezione dei dati di carattere personale" e afferma che "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". Di seguito, il secondo comma enuclea i principi fondamentali. Anzitutto gli obblighi per il *data holder*: "Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge". Quindi i diritti del *data subject*: "Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica". Infine vi è un riferimento alla giusitiziabilità di queste situazioni giuridiche soggettive: "Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Ci troviamo davanti al "rispetto" dovuto all'individuo (entro una sfera privata) con riguardo a intromissioni esterne (articolo 7) e alla protezione della nostra identità, formata dai dati di carattere personale, affidata ad un rapporto giuridico (quindi entro un perimetro relazionale) tra *data subject* e *data holder* (articolo 8). Questi due articoli poggiano su due valori diversi: una forma di libertà negativa il primo, il controllo sui propri dati il secondo; da un lato si è al cospetto di un diritto valido *erga omnes* (articolo 7), dall'altro di una serie di obblighi (lealtà, finalità, base legale) imposti a un soggetto all'interno della suddetta relazione giuridica (articolo 8). Come abbiamo mostrato nella prima parte di questa tesi, per ciò che attiene al primo aspetto la tutela si

concentra principalmente sui fatti "privati", sottratti dalla sfera pubblica, mentre sul fronte della *data protection* l'attenzione si focalizza sui dati di carattere personale che costituiscono la nostra identità nella sfera pubblica. Nel primo caso la dialettica tra interesse privato ed interesse pubblico è il centro del modello di tutela; nel secondo caso, al contrario, tale dialettica si fa evanescente e non viene neppure evocata.

Con riguardo al primo articolo citato, vale richiamare, anzitutto, il principio secondo cui ogni individuo ha diritto a una sfera di libertà personale, grazie alla quale gli è consentito compiere scelte e adottare comportamenti al riparo da intromissioni esterne. Perimetrare questa sfera per valutarne l'estensione vuol dire fare riferimento ai concetti di vita privata, vita familiare, domicilio e comunicazioni[54].

A livello di normativa sovranazionale, il diritto al rispetto della vita privata è stato sancito, subito dopo la fine della seconda guerra mondiale, dall'art. 12 della Dichiarazione universale dei diritti dell'uomo approvata dall'Assemblea generale dell'ONU il 10 dicembre 1948. Tale articolo recita: "Nessun individuo potrà essere sottoposto a interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto a essere tutelato dalla legge contro tali interferenze o lesioni".

Il riferimento all'onore e alla reputazione aggiunge tali aspetti all'elenco già visto *supra*. Si tratta del primo ingresso del concetto di identità nell'area della *hard privacy*: infatti la reputazione non è altro che il riflesso

[54] Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 112.

della nostra identità per come questa è percepita nel contesto sociale nel quale viviamo[55]. Come già anticipato la distinzione è tra informazioni vere (rientranti nell'ambito di tutela della privacy) e tra informazioni false o comunque lesive del decoro e della dignità di un soggetto. Vita privata ed identità sono qui accostate.

La Dichiarazione universale dei diritti dell'uomo, come è noto, riflette un contesto storico segnato dalla fine della seconda guerra mondiale. Negli stessi anni George Orwell pubblica il proprio romanzo più celebre *Nineteen Eighty-Four*[56], titolo ottenuto invertendo le ultime due cifre dell'anno in cui è stato scritto. Tema del romanzo è l'oppressione dei regimi totalitari nei confronti dell'individuo.

A confermare la grande attenzione per la libertà in senso negativo di quegli anni, l'art. 8 della Convenzione europea sui diritti dell'uomo, approvata a Roma il 4 novembre 1950, afferma: "Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una

---

[55] Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 516 e ss. Norberto Nuno Gomes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and articulating Rights*, cit., p. 110.

[56] La pubblicazione è del 1949, ad opera di Secker & Warburg: resta ancora oggi il principale punto di riferimento letterario della privacy verticale: cfr. Neil M. Richards, *Intellectual privacy*, cit., p. 413; Zygmunt Bauman, *Modernità liquida*, Bari, 2000, p. 16; Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 109; Daniel J. Solove, *The Digital Person - Technology And Privacy In The Information Age*, New York University Press, 2004, p. 175.

misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui".

Il richiamo a una sfera di libertà minima è costante ed utilizza ancora i concetti di vita privata e familiare, libertà domiciliare e di comunicazione. Aggiungiamo un ulteriore tassello: la sfera di libertà privata non è assoluta ma può essere limitata in presenza di un interesse pubblico confliggente; la limitazione della libertà privata deve avere base legale, consentendo un controllo democratico di detta compressione, e deve essere necessaria al raggiungimento dell'interesse pubblico, inteso come interesse statuale o interesse collettivo, ossia non deve essere possibile realizzare l'interesse pubblico con altre modalità non invasive della libertà privata.

Si pone dunque un rapporto tra regola generale e regola particolare. La privacy intimità (*hard privacy*), cioè la libertà privata da ingerenze esterne (regola generale), può essere compressa in circostanze eccezionali (regola particolare). Alcuni esempi di interesse pubblico eventualmente prevalente sono: l'interesse alla sicurezza nazionale, all'ordine pubblico, al benessere economico, alla prevenzione dei reati e alla protezione della salute. In tal modo si ottiene una prima indicazione del perimetro privato: i luoghi e i contesti in cui si può e si deve svolgere liberamente la vita privata e familiare.

L'elencazione non è statica ma dinamica, ossia funzionale alla protezione di questa sfera di libertà (la cui protezione è) riconosciuta come diritto fondamentale dall'ordinamento. Questa sfera di libertà è la privacy intimità, individuale e fondamentale, perciò tutelata da un modello di rilievo costituzionale. Gli articoli 14 e 15 della

Costituzione costituiscono il nucleo di riferimento su cui fondare la garanzia della privacy intimità. Il primo (art. 14)[57] riguarda il principio dell'inviolabilità del domicilio, concetto da intendersi come sfera spaziale (*spatial privacy*) di disponibilità esclusiva, il secondo (art. 15)[58] sancisce l'inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione a distanza tra individui. Dalla lettura di ambedue le norme è possibile ricavare la proiezione costituzionale del valore privacy in senso negativo, definendola in termini di inaccessibilità ed esclusività spaziale e conoscitiva di ciò che avviene in determinati contesti in cui si svolge la vita privata e familiare dell'individuo. La sfera pubblica, sia essa sfera statuale o collettiva, dovrebbe arrestarsi dinnanzi alla vita privata, alla vita familiare, all'abitazione e alle comunicazioni degli individui. Il principio costituzionale sopra enunciato si concretizza nella protezione (essenzialmente attraverso norme di natura penale) di quei contesti a tutela della loro inaccessibilità ed esclusività.

---

[57] L'art. 14 della Costituzione italiana afferma che "Il domicilio è inviolabile. Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale. Gli accertamenti e le ispezioni per motivi di sanità e di incolumità pubblica o a fini economici e fiscali sono regolati da leggi speciali". Si tratta dell'attribuzione di un fondamento normativo di rango costituzionale al valore della libertà individuale nella sua accezione di libertà domiciliare.

[58] L'art. 15 della Costituzione afferma che "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge".

L'accessibilità e l'inclusività, per contro, sono caratteri propri di contesti pubblici, nei quali possono ben emergere altri interessi meritevoli di tutela (l'onore, la reputazione, l'identità personale) diversi dalla privacy intimità. Per tali ragioni la privacy di cui ora si tratta è stata definita hard privacy, poiché costituisce il "nocciolo duro" della concezione stessa di libertà.

Pertanto, in linea generale, è possibile affermare che il modello di tutela della *privacy as intimacy* si articola in tre passaggi fondamentali: (i) la vita privata dell'individuo deve svolgersi al riparo da intromissioni esterne; (ii) tali intromissioni possono essere giustificate solo in presenza di un pubblico interesse individuato da una legge; (iii) le misure in cui si concretizza questa intromissione devono essere necessarie (non possono essere sostituite da altre misure meno intrusive) e specifiche (devono essere controllabili) rispetto al perseguimento del pubblico interesse. Definiamo questo modello di tutela *privacy as dignity* perché la regola generale vuole la prevalenza della libertà privata sull'ingerenza pubblica.

Quando parliamo di pubblico in relazione alla privacy intimità pensiamo immediatamente al rapporto tra individuo (portatore, nello schema, di un interesse privato) e Stato (portatore di un interesse pubblico). Lo schema che abbiamo delineato si attaglia ai casi in cui la privacy (intimità) viene sacrificata, ad esempio, per il prevalente interesse pubblico all'accertamento e alla repressione dei reati, chiara prerogativa statuale.

La libertà individuale, sotto questo profilo, si traduce in libertà domiciliare, poiché è il domicilio il primo spazio fisico in cui si realizza l'inacessibilità-esclusività che è caratteristica principale dei luoghi a uso privato. La violazione di domicilio diventa, così, paradigma di una norma penale volta a tutelare la privacy intimità.

La principale distinzione riguarda gli edifici privati – *rectius* ad uso privato – e quelli pubblici – *rectius* ad uso pubblico – come uffici, scuole, ospedali, chiese, cinema. Nel primo caso si tratta di luoghi il cui accesso è precluso alla generalità delle persone, mentre nel secondo caso tali spazi sono aperti alla collettività; i concetti cardine sono quelli dell'accessibilità, della stabilità, ossia della possibilità di intrattenersi per un periodo apprezzabile di tempo al fine di svolgere fatti privati (riconducibili, ad esempio, al lavoro, allo studio e allo svago) e della disponibilità, ossia dell'eventuale potere di accettare o escludere chiunque non sia autorizzato ad entrarvi. La privacy intimità si configura, allora, anzitutto come la proiezione spaziale (*spatial privacy*) degli stessi valori che stanno a fondamento della libertà personale e, quindi, di un diritto umano fondamentale, che può essere compresso in caso di interessi pubblici prevalenti (ad esempio, come già evidenziato, nell'interesse generale all'accertamento dei fatti di reato).

In definitiva, può affermarsi un principio sintetico di portata generale: non è possibile prendere conoscenza di ciò che avviene nella sfera privata domiciliare se non nei casi e nei modi tassativamente previsti dalla legge.

Lo stesso schema sopra descritto trova applicazione alla libertà nelle comunicazioni, quindi ad uno spazio privato in senso metaforico, e quindi al tema, ad esempio, delle intercettazioni[59]. Il bilanciamento di questi due interessi contrapposti (quello privato e quello pubblico) si sostanzia allora nella precisa elencazione dei casi e dei modi con cui l'interesse pubblico, quale regola particolare rispetto alla regola generale, prevale sull'interesse privato.

[59] Neil M. Richards, *Intellectual privacy*, cit., p. 423.

L'equilibrio esistente tra due necessità confliggenti diviene, quindi, l'elencazione delle ipotesi di reato che giustificano lo strumento delle intercettazioni (i casi) e delle modalità con cui il detentore del potere pubblico può intromettersi nell'altrui vita privata (i modi). In particolare, dove tale normativa non ci fosse o non fosse sufficientemente specifica, il rischio del sacrificio del (prevalente) interesse privato della libertà in senso negativo sarebbe troppo alto.

È anche per questa ragione che eventuali violazioni del diritto in capo al soggetto privato così come quelle ai danni del detentore del potere pubblico sono penalmente sanzionate. Ci stiamo riferendo ad un numero nutrito di fattispecie di reato, rinvenibili in quasi tutti gli ordinamenti occidentali a testimonianza dell'universalità dei valori che sono tutelati.

La privacy quale libertà negativa trova così un presidio nel delitto di violazione del domicilio, intendendosi per tale qualsiasi luogo di privata dimora e, dunque, non solo l'abitazione e le sue appartenenze. A conferma del necessario bilanciamento tra interesse privato ed interesse pubblico, il codice penale dedica poi un'autonoma fattispecie, sanzionata più gravemente rispetto a quella generale, all'ipotesi in cui la violazione sia commessa da soggetti investiti della qualifica di pubblico ufficiale. Si tratta di una tutela immediata accordata al precetto costituzionale che stabilisce la compressione dell'interesse privato prevalente solo nei casi e nei modi previsti dalla legge: infatti si afferma la maggiore gravità dei fatti commessi da coloro che, dotati di poteri pubblici, di tali poteri abbiano abusato calpestando l'equilibrio costituzionale tra interesse privato ed interesse pubblico.

Un discorso parzialmente diverso merita il concetto

di corrispondenza e comunicazione. La comunicazione in questo caso è sicuramente intesa come manifestazione della libertà personale e di manifestazione del pensiero riconosciuta dagli articoli 13 e 21 Cost. Il riferimento alla privacy in senso negativo, tuttavia, piuttosto che all'intimità è maggiormente legato alla riservatezza e alla segretezza delle comunicazioni, intesa anche in questo caso come inacessibilità e/o indisponibilità di cose o fatti privati rispetto a un determinato soggetto terzo.

Se la privatezza indica immediatamente e concretamente determinati luoghi in cui si svolge la vita di una persona e, in astratto, una determinata dimensione intima, lo statuto di accessibilità limitata di fatti o informazioni che riguarda le comunicazioni richiama altri concetti che abbiamo già visto essere contigui a quello di privacy. Già abbiamo detto del diritto alla riservatezza; mentre per segretezza si intende ciò che ha un riferimento oggettivo perchè solitamente legato, almeno nel lessico giuridico, all'ufficio, alla professione, all'industria o al commercio.

Ciò che è riservato e segreto, in ogni caso, si caratterizza per il tratto comune di non essere accessibile e disponibile a terzi.

La tutela delle forme di comunicazione a distanza, alla luce delle esigenze sopra enunciate, si concretizza in due modalità: una statica e una dinamica. Sotto il profilo statico sarà vietato prendere cognizione di quanto viene comunicato quando la comunicazione è avvenuta ed è stata registrata su di un qualsiasi supporto; sotto il profilo dinamico, invece, sarà vietato venire a conoscenza di quanto viene comunicato mentre la comunicazione è in corso. Si tratta di due momenti distinti ma nei quali la compressione della libertà individuale è ugualmente evidente. A titolo esemplificativo ma, ovviamente, non

esaustivo, costituisce elemento statico di comunicazione l'e-mail registrata nella memoria del computer del mittente o del destinatario o, ancora, nei rispettivi server. Ciò non dipende dai mezzi di comunicazione a distanza utilizzati, bensì dalla possibilità di qualificare una particolare forma di trasmissione del pensiero come inaccessibile o indisponibile a terzi. Sotto questo profilo rileverà ancora la tutela di una sfera di libertà riconosciuta all'individuo per la manifestazione del suo pensiero e delle sue scelte, con l'avvertenza che può essere l'individuo stesso, nel momento in cui usa uno strumento di comunicazione accessibile e disponibile a tutti (e quindi nel momento in cui pubblica qualche contenuto), a porsi logicamente e giuridicamente al di fuori da questo tipo di ipotesi.

Le nuove tecnologie informatiche hanno, infatti, moltiplicato gli strumenti di comunicazione 'punto a punto' (con cui si trasmette un messaggio da singolo mittente a singolo destinatario) ma anche quelli del tipo 'uno a tanti' (attraverso i quali il messaggio parte da un singolo mittente ma si propaga verso una pluralità di altri soggetti destinatari), ipotesi, quest'ultima, nella quale la comunicazione resta comunque privata se i destinatari sono determinati e determinabili. Tali strumenti, tuttavia, rendono spesso l'informazione pubblica, ossia accessibile a una pluralità non determinata e non determinabile di soggetti. È chiaro che il fuoco della tutela della privacy intimità riguarda solo la prima forma di comunicazione, quella 'punto a punto' o 'uno a tanti determinati', mentre non si occupa della seconda, che, invece, è una vera e propria pubblicazione.

Il modello costituzionale della *privacy as dignity*[60]

[60] Stefano Rodotà, *La vita e le regole*, cit., p. 103.

tutela dunque una certa quota di libertà riconosciuta dall'ordinamento all'individuo attraverso un generale riconoscimento di contesti o ambiti privati (il domicilio, la vita familiare, le comunicazioni) che possono essere compressi solo in presenza di un interesse pubblico prevalente che trae dalla legge il suo riconoscimento e la sua specificazione operativa poiché tale compressione sarà ammissibile nei casi e nei modi previsti dalla legge stessa.

2. Privacy e giornalismo: *privacy as property?*

Nel 1890, Samuel D. Warren e Louis D. Brandeis pubblicarono The right to privacy, opera alla base della quale si pone una tesi semplice ma tutt'affatto che scontata: poiché l'ordinamento già riconosceva il diritto dell'individuo "ad essere lasciato in pace" con riferimento alle eventuali minacce di un male ingiusto provenienti da altri (giustappunto il "*right to be let alone*", l'espressione è del giurista Thomas M. Cooley), questo medesimo diritto avrebbe dovuto giustificare la tutela della tranquillità individuale rispetto alla pubblicazione di fatti privati non connotati da rilevanza pubblica[61]. Il problema di rilevanza pratica che affrontarono i due giuristi era rappresentato dalla stampa ed in particolare dalla stampa scandalistica (la cosiddetta *yellow press*) che faceva uso delle nuovissime macchine fotografiche portatili. Il punto di partenza, com'è noto[62], riguardava la moglie di Warren, Mabel Bayard,

[61] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Georgia Law Journal 123, 2007, p. 129 e ss.

[62] Neil M. Richards e Daniel J. Solove, cit., p. 127; Daniel Solove, *No privacy*, cit., p. 112; Neil M. Richards, *The limits of tort privacy*, cit., p. 361.

figlia del senatore democratico del Delaware Thomas F. Bayard, politico di spicco già candidato alla presidenza degli Stati Uniti e segretario del presidente Cleveland. La stampa di Boston, New York e Washington, con almeno sessanta articoli nell'arco di pochi anni, diede ampia copertura alle vicende, anche tragiche[63], che videro protagonisti i membri della famiglia Warren. L'attenzione dei media per i propri fatti privati portò il giurista a ricercare uno strumento di tutela contro la stampa assetata di "pettegolezzi". Nell'articolo si evidenziava una lacuna normativa particolarmente grave in considerazione delle "minacce" che il progresso tecnologico recava allo *jus solitudinis*[64], vale a dire al pacifico godimento dell'indipendenza privata, massima espressione della libertà dei moderni, come era stata definita nel 1819 dal già citato liberale francese Benjamin Costant.

Si tratta della chiara emersione della privacy quale valore in senso negativo che non aveva ancora trovato proiezione giuridica adeguata rispetto al mutamento tecnologico. Si parla di lacuna normativa, infatti, perché rifarsi alla proprietà privata e alla tutela del proprio domicilio si rivelò non più sufficiente di fronte all'invadenza dei media. Nemmeno il richiamo a una qualche obbligazione contrattuale o quasi contrattuale, come l'obbligo di confidenzialità, risultava utile in

---

[63] Amy Gajda, *What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering The Press Coverage That Led to The Right to Privacy*, in *Illinois Public Law and Legal Theory Research Papers Series*, 2007, p. 9.

[64] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 125; Vittorio Frosini, *L'ipotesi robinsoniana e l'individuo come ordinamento giuridico*, in *Sociologia del diritto*, 2001, p. 5.

relazione a questo specifico problema, limitando così la possibilità per l'individuo di sottrarsi dalla dimensione pubblica e di godersi il massimo bene riconosciuto dalla riflessione filosofica liberale, ossia la propria indipendenza dalla collettività (e dallo Stato)[65].

Con riferimento all'istituto giuridico della proprietà privata, abbiamo richiamato la tutela (anche penale) accordata dall'ordinamento contro le violazioni del domicilio. Concretamente Warren e Brandeis, poggiando sul - già citato - *right to be let alone*, invocarono un'estensione della garanzia accordata al domicilio tramite il riconoscimento di una sorta di diritto di proprietà sui sentimenti privati e sulle emozioni intime[66]. È il concetto di *privacy as property*, riproposto in tempi recenti anche da Zittrain e Lessig[67]. Informazioni private trattate come beni privati, con una conseguenza chiara: essi sono liberamente negoziabili in transazioni economiche (*trade off*) in cui cedere o ritenere le proprie informazioni private presenta dei costi e dei benefici[68]. L'aspetto più interessante di questi studi, al di là del modello teorico di riferimento, è il concetto di *frame*: le transazioni relative

---

[65] John Rawls, cit., p. 14 e ss.; Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 125.

[66] Neil M. Richards, *The limits of tort privacy*, cit., p. 362.

[67] Jonathan Zittrain*, The future of the Internet and how to stop it, Yale University Press*, 2000, p. 200; Lawrence Lessig*, Privacy as property, Social reserch*, 2002, p. 247; Eugene Volokh, cit., p. 1063; Daniel Solove, *No privacy*, cit., p. 34; Lisa Austin, cit., p. 127.

[68] Alessandro Acquisti e Jens Grossklags*, What can behavioral economics teach us about privacy?*, in: Acquisti, Gritzalis, Di Vimercati, Lambrinoudakis (Eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, 2007, p. 363.

alle nostre informazioni, ed in particolare le nostre decisioni riguardo il cedere o il ritenere informazioni private, sono determinate dal contesto, ossia dalla cornice in cui avvengono[69].

Quanto, poi, alla confidenzialità, istituto maggiormente utilizzato nel diritto inglese piuttosto che in quello statunitense, può sostenersi, come fatto da Richards[70], che essa si basi o sulla speciale natura dell'informazione (ad es.: confidenze personali, artistiche e letterarie, segreti commerciali e politici) oppure sullo speciale rapporto di fiducia (trust) tra chi si confida e chi riceve la confidenza (ad es. tra avvocato e cliente, tra medico[71] e paziente). In presenza di un obbligo di confidenzialità, un soggetto ha il dovere di utilizzare i dati in base al contesto e allo scopo della relazione. Un esempio di utilizzo dei dati nel rispetto del contesto è rappresentato dal caso del 1888, Pollard contro Photographic Co., in cui la Corte ha concluso che un fotografo non aveva il diritto di vendere le cartoline di Natale con l'immagine di un cliente a causa della non coincidenza tra il contesto in cui l'utilizzo era consentito e quello in cui, invece, i dati sono stati utilizzati. Un caso in cui, invece, lo scontro si è giocato con riferimento allo scopo per cui i dati sono raccolti è il caso del 1758, Duca

---

[69] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale,* cit., p. 132; Alessandro Acquisti, *Privacy*, cit., p. 324.

[70] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 125; Neil M. Richards, *The limits of tort privacy*, cit., p. 384.

[71] Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, in *Rutgers Law Journal*, 2002, reperibile su Internet all'url http://epic.org/privacy/imshealth/winn_rutgers_02.pdf.

di Queensberry contro Shebbeare, nel quale il giudice, al fine di limitare la diffusione di un manoscritto, ha ritenuto rilevante lo scopo originario, che era diverso dalla pubblicazione. Inoltre, il confidente deve impedire l'accesso a tali dati o la loro divulgazione non autorizzata (nel contesto medico, la riservatezza può essere fatta risalire al IV secolo a.C., quando Ippocrate[72] esortò i colleghi medici a mantenere la riservatezza su quanto rivelato dal paziente nel corso della terapia). Il concetto di *privacy as confidentiality* è, sempre secondo Richards, sottostante alla disciplina europea sulla protezione dei dati personali, come vedremo successivamente.

Possiamo quindi delineare un modello di *privacy as property*, prevalente negli USA, un modello di *privacy as dignity*, prevalente in Europa e alla base della *constitutional privacy* (come abbiamo visto nel precedente paragrafo) e, infine, un modello di *privacy as confidentiality* che permea la regolamentazione della *data protection* (come vederemo nel paragrafo successivo).

Ciò che qui preme sottolineare è che la proposta di Warren e Brandeis di considerare lo *jus solitudinis* in modo analogo alla proprietà privata – quindi come diritto assoluto esercitabile *erga omnes* e non diritto obbligatorio esercitabile nei confronti dell'obbligato – e di tutelare così l'individuo contro le ingerenze esterne divenne il centro della disciplina sulla privacy negli Stati Uniti. Ciò fu possibile anche grazie all'opera di Dean William Prosser[73]

---

[72] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 133.

[73] William Lloyd Prosser, *Privacy*, in *California Law Review*, 1960, p. 388 e 389; Neil M. Richards e Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, in *California Law Review*, 2010; Neil M. Richards e Daniel J. Solove, *Privacy's Other Path:*

che, in un saggio pubblicato nel 1960 sulla California Law Review, sistematizzò la tipologia delle varie violazioni alla privacy, come concepita dai due giuristi bostoniani, attraverso quattro distinte categorie: (1) la (già ricordata) pubblicazione di fatti privati; (2) l'intrusione (*invasion*) in uno spazio privato; (3) il mettere in cattiva luce (*false light*) un soggetto attraverso l'uso di fatti privati e (4) l'appropriazione a fini commerciali del nome o dell'immagine di un privato. Prosser confermò l'impostazione di Warren e Brandeis privilegiando un diritto individuale esercitabile *erga omnes* e tralasciando altri istituti che potevano essere considerati validi strumenti di tutela. L'influenza del *right to be let alone* così concepito fu enorme. Come abbiamo già accennato, il diritto alla privacy si connotò anche in senso costituzionale per consentire all'individuo di sottrarsi dalla sfera pubblica statuale; persino la sentenza della Corte Suprema che negli Stati Uniti ha reso legittimo l'aborto (il celeberrimo caso "Roe *vs* Wade" del 1973, cui si è accennato sopra) si fonda sulla tutela della privacy, intesa come spazio (di decisione) libero da ingerenze esterne (statuali), spazio che pertiene all'inviolabilità della persona, a formare così un'espressione emblematica dei concetti di privacy e di libertà, intrecciati tra loro, in senso negativo.

Il modello proprietario sarebbe così malleabile da consentire la tutela della libertà negativa anche con riferimento alle vicende private. Si focalizza lo strumento (l'istituto giuridico della proprietà) rispetto al valore in gioco (la libertà privata). Anche solo questa considerazione rende la concezione della *privacy as*

Recovering the Law of Confidentiality, cit., p. 148; Neil M. Richards, *The limits of tort privacy*, cit., p. 360.

property come difficilmente accoglibile: il diritto alla privacy è lo strumento di tutela di un valore di libertà in senso negativo, libertà che è uno dei tratti più importanti della dignità di una persona[74]. Tale affermazione riverbera e ha effetto sul modello di tutela nel momento in cui, ad esempio, lo bilanciamo con altri interessi meritevoli di tutela.

Tornando alla prima ipotesi di violazione della privacy (pubblicazione di fatti privati), infatti, risulta evidente il potenziale conflitto tra diritto alla privacy rispetto ad informazioni vere (il *tort privacy* di Warren, Brandeis e Prosser) e la *freedom of expression* (il primo emendamento alla costituzione statunitense)[75]. Proprio dall'analisi del conflitto tra diritti fondamentali, emerge come il modello dalla *privacy as property* sia alla fine irricevibile.

La pretesa di opacità del privato si scontra con l'interesse pubblico alla manifestazione del pensiero e alla trasparenza; emerge l'importanza della distinzione tra ciò che può essere considerato contesto privato e ciò che non lo è; è su questa doppia dicotomia che si concentra il *focus* normativo (interesse privato contro interesse pubblico, da un lato; contesto privato contro contesto pubblico, dall'altro). Emerge, insomma, lo stesso modello di tutela che abbiamo incontrato analizzando la *constitutional privacy* (quindi *privacy as dignity*), ovvero il bilanciamento che ha ad oggetto, allo stesso tempo, la dimensione statuale e quella collettiva e che mira a fissare i limiti dell'una dove l'altra comincia (e viceversa).

---

[74] Ugo Pangallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008, p. 37 e ss.; Neil M. Richards, *Intellectual privacy*, cit., p. 436; Eugene Volokh, cit., p. 1112.

[75] Neil M. Richards, *The limits of tort privacy*, cit., p. 366.

Pertanto avremo la regola generale di prevalenza dell'interesse privato a celare certe informazioni e le regole particolari che, in presenza di un interesse pubblico e quando tali informazioni sono essenziali per il perseguimento di questo interesse, consentono di pubblicare fatti privati ed informazioni personali. La differenza è che la *constituional privacy* poggia su garanzie che si concretizzano in una precisa tipizzazione dei casi e dei modi che consentono l'invasione della privacy, mentra la *tort privacy* non può esaurirsi in una elencazione esaustiva. L'interesse pubblico della notizia e l'essenzialità del dato sono parametri importanti ma non facilmente declinabili in casi e modi di stretta applicazione.

Ancora oggi il cosiddetto diritto all'oblio su Internet, ossia la rimozione di dati personali dallo spazio digitale, può essere invocato solo in assenza di un interesse pubblico prevalente sull'interesse privato (ad es. il diritto di cronaca). In questi termini, la questione si risolve in un problema di qualificazione: ciò che corrisponde all'interesse pubblico (statuale o collettivo) implica che tale dato sia accessibile e pertenga alla collettività; ciò che corrisponde ad un interesse privato implica, al contrario, che il dato venga sottratto alla sfera pubblica. Ci sono quindi dei casi di pubblicazione di fatti privati giustificati dall'interesse pubblico a informare ed essere informati di cui però si fa portatore non lo Stato ma un soggetto privato; in tali situazioni l'aggettivo "pubblico" va interpretato nel senso di "collettivo" (abbiamo parlato di privacy orizzontale). Il soggetto privato, si trova, quindi, a essere portatore di un interesse pubblico (il diritto alla manifestazione del proprio pensiero riconosciuto a livello costituzionale) che prevale sul contrapposto interesse privato.

La dialettica tra Stato e individuo, tipica espressione della concezione di *privacy as dignity*, diviene dialettica tra un individuo portatore di un interesse pubblico collettivo ed un altro portatore di un interesse privato. Questa differenza giustifica, come sappiamo, la distinzione che abbiamo fatto tra privacy verticale e privacy orizzontale all'interno della stessa concezione di fondo, quella della *privacy as dignity*. I comportamenti di carattere intimo e privato non dovrebbero essere soggetti a scrutinio pubblico (sia esso statuale o collettivo) se non nei casi e nei modi stabiliti dalle leggi e secondo le garanzie (diverse per la privacy verticale e la privacy orizzontale) ivi previste. Per illustrare la differenza tra le garanzie poste a tutela della privacy intimità – ed anche per esemplificare il rapporto tra privacy verticale e orizzontale – possiamo trattare il tema delle intercettazioni nell'ambito di un processo penale e della loro pubblicazione. Riprendendo una definizione fatta in precedenza, possiamo parlare di una privacy verticale nel rapporto tra individuo e Stato e di una privacy orizzontale nel rapporto tra privati in cui sia in gioco l'interesse pubblico che abbiamo definito collettivo. Si tratta di problemi da tenere ben distinti: lo si può comprendere facilmente se si pensa, ad esempio, a quanto sia diverso limitare (o ampliare) l'uso delle intercettazioni per finalità di accertamento e repressione dei reati dal limitare (o ampliare) l'eventuale pubblicazione sui giornali delle stesse intercettazioni. In un caso si limita uno strumento di indagine finalizzato all'accertamento e alla repressione dei reati; nell'altro caso si limita la conoscibilità pubblica di fatti emersi nell'ambito di un procedimento penale. Venendo alla regolamentazione di questi problemi chiaramente distinti, occorre verificare, nella prima ipotesi, il rispetto dei casi e dei modi previsti dalla normativa processual-penalistica (le garanzie poste

dall'ordinamento), mentre nella seconda è necessario che le informazioni private contenute nelle intercettazioni siano essenziali (parametro di elaborazione giurisprudenziale e che non può essere facilmente tipizzato) alla finalità informativa che il giornalista intende perseguire. La doppia dicotomia si ripropone, qui, identica: interesse privato *versus* interesse pubblico, essenzialmente identificato nel dovere di accertare e reprimere i reati con il rispetto delle garanzie di legge previste nello Stato di Diritto (cosiddetto *Rule of Law*); di nuovo, privato *versus* pubblico con l'indicazione che possono essere pubblicate solo le informazioni private essenzialmente rilevanti per il raggiungimento e la concretizzazione dell'interesse pubblico ad informare e ad essere informati. La Corte europea ha affrontato un tema analogo in relazione alle intercettazioni casuali – casuali[76] perché disposte contro altro soggetto - subite dal Presidente della Repubblica lituano Rolandas Paksas. Sebbene l'intercettazione di

[76] Come è noto, la Corte costituzionale italiana distingue (sentenza n. 320 del 2007): le intercettazioni «dirette», cioè quelle concernenti utenze riferibili a soggetti garantiti (es. parlamentari) e finalizzate all'ascolto delle sue conversazioni, per le quali la Costituzione e la legge n. 140 del 2003 impongono un'autorizzazione preventiva; le intercettazioni «indirette», cioè attuate riguardo ad utenze non formalmente riferibili al soggetto garantito e tuttavia finalizzate proprio a cogliere le comunicazioni di questi, in base alla notizia di una utilizzazione delle utenze medesime. Anche in questo caso, deve sussistere un'autorizzazione preventiva della Camera di appartenenza; infine le «intercettazioni casuali», cioè quelle che l'Autorità Giudiziaria non dispone intenzionalmente nei confronti del soggetto garantito, e per le quali, proprio per questa ragione, non è concepibile un'autorizzazione preventiva. In questi la richiesta di autorizzazione riguarda solo l'uso delle risultanze.

conversazioni telefoniche costituisse una chiara interferenza nella vita privata del Presidente, tale ingerenza era consentita dalla legge lituana ed era stata autorizzata da un giudice al fine di accertare l'eventuale ruolo del ricorrente nella commissione di un reato. Pertanto la Corte europea giudicò ammissibile l'intercettazione, poiché la legislazione nazionale negava la possibilità di intercettare le telefonate del Capo di Stato, ma non anche le conversazioni in cui lo stesso si trovava a essere l'interlocutore dell'intercettato. Quanto alla pubblicazione delle intercettazioni la Corte europea rilevò che vi era stata una fuga di notizie che aveva effettivamente violato la privacy del Presidente. Tuttavia quando lo stesso venne messo sotto accusa e le intercettazioni vennero pubblicate nell'ambito del procedimento avanti la Corte costituzionale trasmesso in diretta televesiva, non vi fu alcuna violazione della privacy: si trattava di informazioni di indubbio interesse pubblico. La Corte europea ha poi evidenziato che le figure politiche di spicco sono inevitabilmente soggette al controllo dei media, il cui ruolo è necessario per garantire il diritto all'informazione della collettività. Pertanto, la pubblicazione di queste conversazioni non è stata considerata lesiva dei diritti contenuti nella Convenzione Europea sui Diritti dell'Uomo[77].

E' chiaro che questo interesse alla manifestazione del pensiero prevale sul diritto alla vita privata solo se concretizza effettivamente detto interesse pubblico e dunque la pubblicazione di dati riservati è necessaria al conseguimento di questo superiore interesse. Riteniamo

[77] Giulio Garuti, *Intercettazioni telefoniche e politica in Lituania*, Dir. Pen. e Processo, 2012.

quindi che lo schema delineato in precedenza sia ugualmente valido e applicabile anche a questa ipotesi: solo che mentre nella privacy verticale avremo base legale ed elencazione dei casi e dei modi che giusitificano la compressione della privacy negativa, nella privacy orizzontale avremo sempre una base legale (un principio costituzionale come la "*freedom of expression*") e un parametro di necessarietà (o essenzialità) della pubblicazione dei dati privati per il raggiungimento dell'interesse pubblico[78].

La regola generale, dunque, è che i giornalisti non devono fornire notizie o pubblicare immagini di soggetti coinvolti in fatti di cronaca salvo che non sia possibile ravvisare la rilevanza sociale della notizia o dell'immagine. Nel caso in cui tale pubblico interesse vi sia, il giornalista può e deve pubblicare solo quei dati che sono essenziali per la realizzazione della finalità pubblica.

In relazione ai personaggi pubblici occorre fare una precisazione: i protagonisti dello spettacolo, della politica, dello sport e in genere le persone note hanno una sfera privata circoscritta, nel senso che il loro ruolo pubblico giustifica la pubblicità delle informazioni che li riguardano e che siano pertinenti con tale ruolo.

Quindi la loro libertà privata deve essere in ogni caso rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica. Ad esempio: se una

[78] I principi fondamentali qui espressi sono presenti nella giurisprudenza della Cassazione sia civile (Corte di Cassazione sez. un., 27 maggio 1999, n. 318; Corte di Cassazione sez. III, 9 giugno 1998, n. 5658) sia penale (Corte di Cassazione, 30 giugno 1984, n. 8959): in queste pronunce si legge che il diritto di cronaca prevale sul diritto alla privacy se i fatti sono veri, di interesse pubblico e se sono esposti in forma corretta.

pattuglia di vigili urbani ferma un'auto con un *viado* che si accompagna a un esponente politico in piena campagna elettorale, in cui uno dei punti qualificanti è una serrata battaglia contro la prostituzione extracomunitaria, può e deve essere lecito pubblicare il nome del politico perché questo fatto ha una diretta attinenza con il suo ruolo di personaggio pubblico[79]. Parallelamente, in un'indagine sullo sfruttamento della prostituzione, i dati identificativi di un giornalista sportivo non sono stati considerati pubblicabili perché, in questo caso, il fatto non era pertinente rispetto al ruolo pubblico del protagonista. Ovviamente un personaggio che riveste una posizione di particolare rilevanza pubblica può godere di una libertà privata inversamente proporzionale alla sua notorietà e al suo ruolo, con riferimento anche agli ambiti maggiormente riservati, ossia la salute, la sfera sessuale o l'orientamento politico dell'individuo. Come ha osservato la Corte Suprema americana nel caso New York Times contro Sullivan[80], il dibattito democratico richiede la possibilità di attaccare in modo veemente, caustico e a volte sgradevole i personaggi pubblici in relazione al ruolo da loro rivestito nella società[81].

Un minore, al contrario, gode di una tutela rafforzata della propria intimità, proprio in considerazione dei rischi legati alla diffusione incontrollata di fatti che li riguardano e dei possibili danni che potrebbero subire.

Esistono anche casi limite: a tal proposito vale menzionare la vicenda giudiziaria che ha visto coinvolti

---

[79] Mauro Paissan (a cura di), *Privacy e giornalismo*, Roma, 2008, p. 17 e ss.
[80] 376 U.S. 254, 270 (1964).
[81] Neil M. Richards, *The limits of tort privacy*, cit., p. 372.

Naomi Campbell e il Daily Mirror[82]: nel 2004, infatti, la top model ha vinto una causa contro il noto quotidiano scandalistico, condannato al pagamento di 3,500 sterline per aver pubblicato le foto scattate alla star mentre lasciava un incontro di recupero per tossicodipendenti dalla sede del centro in King's road nel quartiere di Chelsea, a Londra. La sentenza, ribaltata in appello ma poi confermata in ultimo grado, recita: "*It is not only a vindication for her personally but, more importantly, represents a real advantage for the rights of people to maintain important elements of their privacy, particularly when related to therapy and people who need to have treatment*". La condanna del giornale si basa sull'infrazione della *confidentiality* nonché dei doveri derivanti dal Data Protection Act del 1998 (le foto risalivano al 2001). Il caso è un esempio eccellente di quanto sia difficile conciliare il diritto alla riservatezza con il diritto di cronaca, in questo caso giornalistica. La tendenza a privilegiare il rispetto di questioni particolarmente delicate inerenti la sfera privata di soggetti pur abituati a stare sotto i riflettori è qui stata ufficialmente inaugurata, anche se non può certo affermarsi che si sia sviluppata in modo omogeneo, né nel Regno Unito né altrove; piuttosto, al contrario, si è assistito ad un'inversione di rotta, culminata nella controversa vicenda riguardante Lady Diana, cui qui si accenna solamente, rimandando a quanto noto ai più.

Riprendendo, quindi, il nostro schema, si avrà che: (i) la vita privata dell'individuo deve svolgersi al riparo da intromissioni esterne; (ii) tali intromissioni possono essere giustificate solo in presenza di un pubblico interesse; (iii)

[82] http://news.bbc.co.uk/2/hi/uk_news/3689049.stm

la forma in cui si manifesta questa intromissione deve essere necessaria e specifica (essenziale) rispetto al raggiungimento del pubblico interesse[83].

Il modello proprietario di tutela della privacy non è in grado di spiegare adeguatamente il suddetto schema, che, peraltro, applicato alla privacy orizzontale vede, come abbiamo già evidenziato, un'importante differenza: mentre, infatti, è certamente possibile individuare una base legale sia in merito alla privacy verticale (per esempio in materia di intercettazioni) sia in merito alla privacy orizzontale (per esempio in materia di attività giornalistica dove la base legale può essere il diritto costituzionale alla manifestazione del pensiero), non può dirsi che per la privacy orizzontale vi sia una chiara e inequivoca elencazione dei casi e dei modi in cui una compressione della libertà individuale possa essere considerata ammissibile. A tale carenza normativa ha provveduto inizialmente la giurisprudenza, elaborando una serie di criteri che forniscono le linee guida in materia: si tratta di regole analoghe a quelle vigenti in caso di lesione dell'onore e in materia di protezione dei dati personali. In particolare, come già scritto, si è stabilito che i fatti narrati devono essere pertinenti ed essenziali rispetto all'interesse pubblico perseguito.

Vi è poi un altro argomento per sostenere l'inadeguatezza del modello proprietario: il carattere dinamico della concezione della *privacy as dignity* rispetto al carattere statico della concezione della *privacy as property*. Con la loro opera, Warren & Brandeis fornirono una risposta in termini di configurabilità di un "*tort*" in caso di pubblicazione non autorizzata di fatti privati. Tale

[83] Neil M. Richards, *The limits of tort privacy*, cit., p. 375.

azione equivaleva ad una sorta di minaccia. Per questo presero in prestito da Cooley l'espressione "*right to be let alone*" (nel libro The Law of Torts del 1888)[84]: intendevano indicare l'interesse privato preponderante, a loro giudizio, sull'interesse collettivo alla pubblicazione di notizie. Le loro riflessioni poggiavano su un'estensione del concetto di proprietà privata basata sulla distinzione oggettiva tra contesto pubblico e contesto privato, distinzione antica di tremila anni e che avrebbe limitato l'invadenza dei media. I sentimenti privati dovevano restare privati, non disponibili per altri salva la possibilità di autorizzazione dell'individuo. Nell'impatto con il diritto alla manifestazione del pensiero occorre chiedersi se è possibile tracciare il perimetro di ciò che è privato, cioè la sfera oggetto di tutela immediata della privacy intimità. Nella tradizione giuridica sopra citata con riferimento alla privacy verticale cogliamo un richiamo costante a tre ambiti (vita familiare, domicilio e corrispondenza-comunicazione) entro cui dovrebbe garantirsi una sfera di libertà di scelta e di comportamenti personali che sono diretta espressione della libertà in forma negativa. Questa sfera di espressione deve essere protetta in maniera non statica bensì dinamica, ossia in rapporto funzionale con la libertà che l'ordinamento vuole garantire. Se tale argomento è valido con riferimento alla privacy verticale, a maggior ragione deve essere tenuto in debito conto per la privacy orizzontale. Ogni avanzamento tecnologico che porta a moltiplicare le ipotesi d'intromissione nei (e di conseguente divulgazione di) fatti privati richiede un nuovo equlibrio tra interesse privato e interesse pubblico.

---

[84] Neil M. Richards e Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, cit., p. 1892.

Ciò equivale a dire che tutto quanto non è ricompreso nella base legale e non sia essenziale al perseguimento di un interesse pubblico (privacy orizzontale nel caso della pubblicazione di fatti privati) o non rientri nella chiara elencazione dei casi e dei modi in cui opera un'eccezione alla libertà privata (privacy verticale) dovrebbe essere vietato a prescindere dalla individuazione statica di precisi perimetri privati. Ragionare diversamente, d'altra parte, vorrebbe dire lasciare l'individuo in balìa di confini mai certi, vittima della dialettica tra dimensione pubblica e dimensione privata, dovendosi qui intendere per privato ciò che viene sottratto dalla dimensione pubblica, cioè quella dimensione che riguarda la società nel suo complesso (e che in senso patologico diviene pressione sociale sull'individuo) o nelle sue articolazioni politiche (la cui degenerazione consiste, invece, nell'oppressione politica sulla persona)[85]. In presenza di confini permeabili e di una concezione statica dei contesti privati, è evidente che la pressione sociale e l'oppressione politica sono destinate a prevalere. Il parametro di riferimento è sempre e comunque la quota di libertà che viene garantita all'individuo, piuttosto che la proprietà che egli può esercitare sulle proprie informazioni personali. Sia con riferimento alla sorveglianza, sia con riferimento al diritto alla manifestazione del pensiero, si tratta pur sempre di un problema di libertà più che di un problema di proprietà. Come abbiamo osservato nel primo capito: qual è il grado di controllo che gli altri possono esercitare sull'individuo? Questa è la domanda fondamentale che lascia trasparire un valore comune (privacy in senso negativo) sia per la

[85] John Rawls, cit., p. 304; Asa Briggs e Peter Burke, *Storia sociale dei media*, Bologna, 2010, p. 90 e ss.

privacy verticale analizzata nello scorso paragrafo sia per la privacy orizzontale analizzata in questo paragrafo.

La privacy intimità viene quindi tutelata in termini di *privacy as dignity* più che di *privacy as property*.

3. Privacy e banche dati: *privacy as (new) confidentiality*

È luogo comune considerare la *grundnorm* della privacy la Convenzione di Strasburgo (adottata nel 1981) sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, dalla quale poi hanno tratto orgine le varie direttive europee in materia di *data protection*. Occorre, allora, verificare se anche in relazione alla disciplina sulla *data protection* la domanda fondamentale sia quale livello di controllo gli altri sono in grado di esercitare sull'individuo, ossia se il valore fondamentale tutelato da tali norme sia la (privacy intesa come) libertà in senso negativo, e, ancora, se la concezione migliore per descrivere il relativo modello di tutela sia quello della *privacy as dignity*. La risposta a entrambe le domande è no.

Le regole poste a tutela della *privacy as dignity*, da una parte all'altra dell'Atlantico, sono l'insieme delle garanzie individuali di non essere sottoposti a perquisizioni e sequestri ingiustificati da parte del governo e, specularmente, di assumere alcune decisioni al riparo da intromissioni non giustificate[86]. Si tratta della possibilità di

[86] Con particolare riferimento agli Stati Uniti, si tratta delle decisioni in tema di contraccezione, aborto e altre fondamentali questioni come il matrimonio, la procreazione, l'educazione dei figli e l'istruzione. I valori sottesi sono, tra gli altri: la solitudine, l'intimità (il desiderio di limitare l'accesso a un luogo o a una dimensione di vita), la riservatezza e la sicurezza: vedi Jean Cohen,

agire e prendere decisioni liberamente e al riparo dall'altrui controllo, senza che il potere politico o l'opinione pubblica possano fungere da limite.

Storicamente, tuttavia, assistiamo all'emergere di un altro insieme di regole che costituisce un altro e diverso modello di regolazione della privatezza. La vita dell'individuo diviene riproducibile, comunicabile, sorvegliabile, memorizzabile con strumenti sempre nuovi e sempre più potenti.

La privacy intimità, la hard privacy, ha un preciso ancoraggio normativo: è una libertà riconosciuta a livello nazionale e sovranazionale che si lega ai concetti di vita privata, di famiglia, di domicilio e di strumenti di comunicazione a distanza e punto a punto. Il pubblico, statuale o collettivo, può limitare tale libertà. La limitazione di tale libertà di azione, di scelta, di comportamento è presidiata da alcune garanzie giuridiche stabilite a livello costituzionale e consacrate in fattispecie penali. Abbiamo visto che queste garanzie si atteggiano in maniera diversa a seconda che si parli di privacy verticale (rapporto con il potere pubblico statuale) o orizzontale (rapporto con il potere pubblico collettivo). Le norme assicurano una quota di libertà in questi contesti (vita privata, vita familiare, domicilio e comunicazioni) perché questi contesti, intesi in senso dinamico e funzionale, possono essere definiti, in base ad una tradizione assai risalente nel tempo, come contesti privati. Allo stesso modo, i contesti pubblici (quelli riguardanti l'azione dello Stato o gli interessi della collettività) sono caratterizzati (o dovrebbero essere caratterizzati) da un'ampia

---

Regulating Intimacy: A New Legal Paradigm, Princeton, 2002, p. 57; Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 553 e ss.

accessibilità/conoscibilità. I conflitti riguardano quindi il passaggio da generalmente "accessibile" (pubblico) a generalmente "non accessibile" (privato) e, in senso inverso, da "non accessibile" ad "accessibile".

Si tratta di concetti tradizionali, sia dal punto di vista giuridico che filosofico. Tuttavia la distinzione tra pubblico e privato entra in crisi nel momento in cui si moltiplicano i dati potenzialmente a disposizione e la possibilità di accesso a tali dati diviene un fattore pervasivo della nostra società. L'ipertrofia e l'iperaccessibilità dei dati diviene elemento non facilmente inquadrabile nella dicotomia privato/pubblico[87]. Si pensi, ad esempio, alla presenza di telecamere di sorveglianza davanti agli edifici o negli spazi condominiali. Oppure alle nuove possibilità offerte dai servizi di ricerca che utilizzano dati raccolti attraverso i social network (cosiddetta *social search*). Sarà possibile cercare qualsiasi contenuto condiviso, sia esso una foto, un video o un post. Se per caso viene condivisa la foto in un esercizio pubblico con geolocalizzazione, quella foto diviene ricercabile da chiunque scriva il nome di quell'esercizio pubblico o di un luogo di interesse nei pressi.

Ed è in quest'ambito che si inserisce il concetto di anonimato, da intendersi da un lato come il massimo grado di privacy concepibile, ovvero una sorta di "diritto a non essere nessuno", dall'altro come prerogativa individuale di riservatezza rispetto al grado di diffusione dei propri dati personali e alle modalità della loro circolazione. Nell'era del web è molto difficile rifugiarsi nell'anonimato, tutto è

[87] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 88 e ss.; Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 537 e ss.; Marit Hansen, cit., p. 199; John Palfrey e Urs Gasser, *Nati con la Rete*, Milano, 2009, p. 378.

tracciato o rintracciabile; ogni informazione è registrata, elaborata, trasmessa e archiviata. Può però intervenirsi sulla protezione di tali informazioni da abusi e diffusione abnorme o più semplicemente ingiustificata, perché non legata allo scopo per cui il dato è stato comunicato dall'avente diritto. È decisamente sposando questa seconda accezione che ci si riferisce all'idea di anonimato, cercando di includerla nei valori-guida cui il legislatore dovrebbe ispirarsi per garantire una tutela rotonda e completa dell'individuo lasciandogli totale libertà di espressione e comunicazione, senza che ciò incida dannosamente sulla propria identità.

Dall'inizio del 1960, l'aumento della raccolta, della registrazione e dell'analisi di dati personali a seguito dello sviluppo delle nuove tecnologie informatiche aveva permesso a pubbliche amministrazioni e imprese di migliorare la loro efficienza e la loro produttività, sollevando tuttavia preoccupazioni riguardo l'(ab)uso di questi dati. Il timore che fosse il potere pubblico statuale ad abusare dell'enorme mole di informazioni mano mano raccolte rimandò immediatamente al concetto di privatezza come limite all'ingerenza dello Stato. Le preoccupazioni erano più che giustificate: durante la Seconda Guerra Mondiale, la Germania nazista era entrata in possesso di dati personali dei cittadini delle nazioni che venivano invase. Più tali informazioni erano accurate più agevolavano la persecuzione di ebrei e zingari. La percentuale di olandesi (73%), belgi (40%) e francesi (25%) perseguitati dal regime variò proprio in funzione dell'accuratezza di queste informazioni[88]. Nel 1969 in

[88] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 141; Francesca Bignami, cit., p. 610.

Svezia vi fu una forte opposizione al censimento che avveniva per la prima volta in maniera completamente automatizzata, ingenerando preoccupazioni sull'analisi dei dati e sul loro uso da parte del potere politico per schedare (e quindi controllare e manipolare) i cittadini. Il governo, sotto pressione per le accuse dell'opposizione, istituì una commissione per studiare il fenomeno e suggerire iniziative legislative. Nel 1970, lo Stato tedesco dell'Assia (Hesse) adottò il primo atto legislativo al mondo rivolto specificamente al trattamento automatizzato dei dati, ossia un "Data Protection Act" che trovava applicazione ai dati raccolti dalla pubblica amministrazione. La legge istituiva un commissario per la protezione dei dati sotto l'autorità del parlamento dello Stato il cui compito era quello di garantire la corretta conservazione, trasmissione e utilizzazione delle informazioni. In quegli anni[89] la Svezia (1973), seguita dagli Stati Uniti (1974), dalla Repubblica federale di Germania (1977) dalla Francia (1978) e dalla Gran Bretagna (1984), adottò una serie di provvedimenti, veri e propri "*Data acts*", per impedire la diffusione di banche di dati segrete e l'uso "secondario" di tali dati memorizzati negli archivi informatici, "secondario" perché ulteriore rispetto alla finalità primaria del trattamento (il cosiddetto *secondary use*). Questi provvedimenti si applicavano sia al settore pubblico sia al settore privato e fissavano alcuni principi cardine: la vigilanza sull'applicazione della normativa era affidata ad una

[89] Helen Nissenbaum, *Privacy as contextual integrity*cit., p. 108; Daniel J. Solove e Chris Jay Hoofnagel, *A Model Regime Of Privacy Protection*, cit., p. 360 e ss.; David H. Flaherty, *Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies*, in *Science, Technology & Human Values*, 1986, p. 8.

autorità indipendente in grado di vigilare su eventuali abusi (in particolare del potere pubblico statuale); l'interessato aveva il diritto di essere informato in merito a tutti i trattamenti che venivano effettuati e, salvo che il trattamento non fosse previsto da una legge, nessun nuovo trattamento dei dati poteva essere effettuato senza il consenso del soggetto; l'interessato aveva il diritto di accedere gratuitamente ai dati che lo riguardano; se i dati riportavano informazioni inesatte o incomplete, questi dovevano essere corretti ed aggiornati. Un insieme di regole per la corretta gestione delle banche dati, inizialmente poste quale argine al potere pubblico nei confronti del privato in caso di archiviazione di dati che lo riguardavano; in sintesi: *data base privacy*.

Successivamente l'OCSE emanò le Linee guida sulla protezione dei dati e sui flussi transfrontalieri di dati personali (1980) e il Consiglio d'Europa approvò la già ricordata Convenzione per la protezione delle persone rispetto al trattamento automatizzato dei dati personali (1981). La Convenzione ha dichiarato che "è auspicabile estendere la protezione dei diritti di ciascuno e delle libertà fondamentali, e in particolare il diritto al rispetto alla vita privata, tenendo conto del flussi internazionali di dati personali oggetto di trattamento automatico".

Il riferimento è al rispetto della vita privata: il valore tutelato è la libertà in senso negativo. Tuttavia quello che non convince è che il riferimento alla qualificazione "privata" è del tutto pleonastico: oggetto di tutela, come più volte ricordato, non sono i nostri dati privati, bensì più ampiamente le nostre informazioni personali; l'archiviazione e la trasmissione di queste informazioni non tengono in conto il contesto privato e pubblico, se non con riferimento, come vedremo, alla base legale del trattamento. Ciò detto, una volta che sia esclusa la

possibilità di sottrarsi dal trattamento dei dati e quindi dalla relazione (si pensi all'esempio dei rapporti tra cliente ed istituto di credito, tra medico e paziente, tra utente e Internet Service Provider), attribuiamo valore alla *data protection* perché tale disciplina è posta a tutela della nostra identità contestuale, ossia delle informazioni personali che ci riguardano e che sono condivise in un certo contesto.

In sintesi: quando vi è *data sharing* la protezione dei dati personali consente di determinare come questa condivisione deve avvenire.

Le violazioni della *data protection* sono, come anticipato, delle decontestualizzazioni in senso sincronico o diacronico. Gli otto principi stabiliti dall'OCSE in quello che è il primo Global Privacy Standard sono: (i) il principio di limitazione, che stabilisce che i dati personali devono essere raccolti in modo lecito ed equo e, se possibile, con il consenso della persona interessata; (ii) il principio di "*data quality*", che stabilisce che i dati personali devono essere pertinenti alle finalità per le quali sono stati raccolti e, in relazione a tali finalità, devono essere accurati, completi ed aggiornati; (iii) il principio di finalità, che stabilisce che gli scopi per cui sono raccolti i dati personali devono essere specificati al momento della raccolta dei dati ed il successivo utilizzo deve essere sempre coerente rispetto a tali scopi; (iv) il principio di salvaguardia, che stabilisce che i dati devono essere protetti da misure di sicurezza ragionevoli contro i rischi di perdita, distruzione, accesso ed uso; (v) il principio di accessibilità, che stabilisce che il *data holder* adotti una *policy* generale di trasparenza riguardo i trattamenti di questi dati, dovendosi dare visibilità all'esistenza e alla natura dei dati personali trattati, oltre che agli scopi principali del loro uso; (vi) il principio di partecipazione

individuale, che stabilisce che una persona dovrebbe avere il diritto di conoscere l'identità del *data holder*, di accedere gratuitamente e facilmente ai dati da lui detenuti, di ottenere riscontro alle richieste di informazione e correzione relativa ai propri dati personali e di ottenere, in determinati casi non ben precisati, la cancellazione dei dati; (vii) il principio di responsabilità, che stabilisce la responsabilità del *data holder* chiaramente individuato riguardo le eventuali violazioni e in particolare riguardo la mancata adozione delle misure di sicurezza volte ad evitare la perdita, la distruzione e l'alterazione delle informazioni e l'accesso non autorizzato alle banche di dati. Analizziamo la declinazione giuridica di questi principi: chiunque ha diritto alla protezione dei dati personali che lo riguardano. Tale diritto si basa su una serie di obblighi (per quanto ci riguarda assimilabili a un generale obbligo di confidenzialità e ad un dovere di trasparenza) imposti al soggetto che tratta i dati (*data controller* o titolare del trattamento dei dati) attraverso la loro gestione in banche di dati, da intendersi come un complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti. Il trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali del *data subject*, ossia della persona fisica a cui si riferiscono i dati.

L'ambito d'applicazione e il cuore della normativa è (i) il trattamento (ii) di dati personali (iii) per una certa finalità. La normativa nazionale si applicherà a chiunque è stabilito nello Stato oppure impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito.

Quanto alla nozione di (i) trattamento, essa è molto ampia: l'art. 4 lett. a del Codice Privacy italiano considera

tale “qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati”. Il Codice fornisce poi delle definizioni per singoli trattamenti, ritenuti particolarmente significativi, ossia per la comunicazione (il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione); per la diffusione (il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione); per il blocco (la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento).

Quanto alla nozione di (ii) dato personale, esso è, come noto, qualunque informazione relativa a persona fisica identificata o identificabile. Non è dato personale, all’evidenza, quello anonimo, ossia quello che, in origine o a seguito di trattamento, non può essere riferito a un interessato identificato o identificabile. Premessa la distinzione tra dato personale e dato anonimo, occorre ulteriormente distinguere i concetti di dati identificativi, dati sensibili e dati giudiziari. I dati identificativi sono i dati personali che permettono l’identificazione diretta dell'interessato; i dati sensibili sono quelli idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche,

l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; i dati giudiziari, infine, sono i dati personali idonei a rivelare l'esistenza di precedenti giudiziari o comunque la pendenza di procedimenti penali a carico del *data subject*.

Quanto alla nozione di (iii) finalità, il titolare del trattamento dovrà articolare e specificare la finalità o le finalità per cui sono raccolti i dati personali al più tardi al momento della raccolta dei dati. Occorre tuttavia distinguere finalità personali e finalità non personali. In caso di finalità esclusivamente personali, il trattamento di dati personali effettuato da persone fisiche non è soggetto all'intero *corpus* normativo. È fatto salvo, come già anticipato, il caso in cui i dati siano destinati a una comunicazione sistematica o alla diffusione.

Nonostante l'origine della normativa risieda, come visto, nella dialettica privato/pubblico o, meglio, nel timore che il potere pubblico potesse abusare di banche dati segrete[90], il *focus* è evidentemente il trattamento di dati personali (non più dati privati[91]) che deve svolgersi nel rispetto di determinati obblighi (prescindendosi completamente da un interesse pubblico se non nei casi in cui è una legge a stabilire la base legale del trattamento dei dati).

Sfuma dunque la dicotomia tra privato e pubblico, importante solo per stabilire l'ancoraggio della base legale del trattamento: in ambito privato è generalmente richiesto

[90] Manuel Castells, *Galassia internet*, Milano, 2006, p. 168 e ss.
[91] Sul rapporto tra dati sensibili e dati privati: Lisa Austin, cit., p. 153.

il principio di consenso alla base – legale, s'intende – del trattamento stesso; in ambito pubblico, solitamente, il trattamento dei dati avviene in forza di una legge.

Non può dirsi quindi che il valore di riferimento sia la privacy in senso negativo, il valore di questa normativa è piuttosto la privacy in senso positivo: non si tratta più della libertà dall'essere controllati ma della libertà di controllare le proprie informazioni personali, quella libertà, cioè, di cui parlava Westin. Non più, ancora, di qual è il grado di controllo che gli altri possono esercitare nei confronti dell'individuo, piuttosto di qual è il grado di controllo che l'individuo può esercitare sui propri dati personali.

Abbiamo quindi la piena manifestazione delle due teorie della privacy-valore descritte nel primo capitolo: quella tradizionale e negativa, la *hard privacy*, e quella moderna e positiva, la *soft privacy*. *Soft* perché il problema non è più se condividere informazioni su di sé ma come e con chi condividerle; *soft* perché quando si affrontano problemi in cui le due teorie sono sovrapposte sarà sempre lei a cedere. Inutile aggiungere che tutte le volte che vengono confusi questi due livelli, vengono confusi anche i modelli di tutela. Questa sovrapposizione non giova a chiarire quali regole debbano essere applicate per realizzare il valore sottostante: nella *data protection*, dovrebbe essere l'identità personale contestuale. Ogni individuo ha diritto di determinare la propria identità e quindi di controllare la circolazione dei dati personali che lo riguardano entro un determinato contesto.

Come? Nella *data protection*, lo strumento di tutela di tale diritto è l'imposizione di obblighi sul *data holder* quale tutela "a monte" del diritto di controllare la circolazione dei dati. Rispetto al diritto a vedere tutelata la propria vita privata, familiare e le proprie comunicazioni si

pongono situazioni giuridiche diverse che possono (ma non devono) parzialmente coincidere: valori sottesi diversi (non solo privacy negativa, ma anche ed in maniera decisiva tutela dell'identità personale), contenuto giuridico diverso (controllo che si declina in obblighi di trasparenza, base legale ed adozione di misure di sicurezza), oggetto di tutela diverso (dati personali).

Siamo oltre la distinzione tra pubblico e privato: concettualmente, infatti, l'idea che la privacy (valore) possa essere in qualche modo violata in uno spazio pubblico è paradossale. Eppure la *data protection* affronta anche questo genere di situazione, imponendo obblighi di limitazione, di trasparenza, di salvaguardia. Abbiamo visto che la *hard privacy* si basa sulla tutela di contesti privati (il domicilio, i mezzi di comunicazione) per dare sostanza ai termini di vita privata e vita familiare: la vita privata (e/o la vita familiare) è quella che si svolge in quei contesti. La *data protection* amplia e moltiplica i contesti rilevanti: tutte le relazioni tra *data holder* e *data subject*, nel momento in cui il secondo raccoglie ed usa i dati personali del primo, pongono delle regole e dei limiti.

Il problema, tuttavia, oltre ad essere qualitativo (diverso oggetto di tutela, diverso contenuto normativo) è quantitativo: le informazioni che riguardano le persone, indipendentemente dal loro statuto pubblico/privato, sono diventate un bene sempre più prezioso, non solo nell'esercizio delle prerogative statuali ma anche nell'esercizio di attività economiche, professionali e commerciali. Con la conseguenza che il bilanciamento tra interessi contrapposti (rendere o meno accessibile quell'informazione) diventa assai più frequente che i casi di conflitto tra pubblico e privato che danno sostanza alla *constitutional* e alla *tort* privacy, ossia in definitiva alla privacy verticale e a quella orizzontale. Non ci si concentra

più solo sull'uso delle intercettazioni nei procedimenti penali, né sulla pubblicazione delle foto in spiaggia di qualche personaggio famoso, bensì sull'uso di Internet che viene fatto quotidianamente per molte ore al giorno da miliardi di persone.

La vita di relazione che si svolge anche grazie agli strumenti tecnologici, d'altronde, rende fluidi e permeabili i confini delle due sfere classiche, quella privata e quella pubblica. La sfera sociale si arrichisce di un nuovo contesto, né privato né pubblico: anzi, il pubblico diventa privato ed il privato diventa pubblico. I concetti di accessibilità e indisponibilità, così importanti per delineare la quota di libertà riconosciuta da un ordinamento, sono anch'essi più sfumati, meno certi, dinnanzi alla capacità di trasmettere e condividere grandi quantità di informazioni attraverso Internet, la capacità di aggregare informazioni in database di grandi dimensioni, la riduzione dei costi di archiviazione dei dati e l'aumento della potenza di elaborazione. Non ci sono limiti tecnologici alla quantità di informazioni circolanti, informazioni che sono registrate, analizzate e condivise con facilità da soggetti sparsi in tutto il mondo.

Questa sfera sociale è costituita da un numero elevatissimo di interazioni tra un *data subject* ed un *data holder*. La *data protection* dovrebbe garantire tutela al *data subject* rispetto all'archiviazione e alla circolazione dei dati che lo riguardano. Questa zona intermedia, né privata né pubblica, dove freneticamente circolano le informazioni, aumenta giorno dopo giorno. La *spatial privacy*, la *hard privacy*, la privacy intimità non sono in grado di rispondere alle varie e multiformi esigenze di tutela del *data sharing*.

Il punto ora è rispetto a che tipo di violazioni si pone tale esigenza di tutela. Serve un riferimento più malleabile

che quello di contesto privato (la famiglia, il domicilio, le comunicazioni punto a punto) contrapposto al contesto pubblico.

Riteniamo che la *data protection* riguardi essenzialmente un contesto di relazione e che questa sia una grande differenza con il diritto alla privacy inteso quale diritto individuale esercitabile *erga omnes*. Ogni relazione tra *data holder* e *data subject* è calata in un contesto: per questo il valore che si realizza consiste nella tutela dell'identità contestuale, ossia dell'insieme di dati personali (identità) in riferimento ad un certo contesto (contestuale) in cui avviene lo scambio di informazioni. Detto altrimenti: le informazioni di ciascuno vengono comunicate e quindi sono accessibili in relazione al contesto nel quale circolano e al rapporto tra *data subject* e *data holder*. Diventa, così, nuovamente centrale il concetto di relazione; tanto è vero che è possibile ricostruire il diritto alla protezione dei dati personali anche utilizzando uno schema giuridico diverso.

Infatti, è possibile perseguire i valori della privacy positiva e dell'identità personale anche facendo ricorso ad altri istituti giuridici: ad es. nel rapporto di confidenzialità, il confidente ha obblighi simili al *data holder*.

Nel viaggio a ritroso nel tempo emerge un parallelismo interessante: Warren e Brandeis "inventarono" un generale diritto alla privacy (1890) proprio per l'inadeguatezza di una tutela dei fatti privati (non pubblici) basata esclusivamente sul rapporto di confidenzialità. Siccome poteva non esserci un rapporto giuridico sottostante e quindi poteva non esserci alcun rapporto di confidenzialità, era indispensabile forgiare un nuovo diritto di carattere generale e individuale (non

legato a un rapporto giuridico)[92]. Negli anni '70, tuttavia, il problema centrale era quello dei *data base* e dei *data holder* che raccoglievano, memorizzavano ed analizzavano dati personali che venivano forniti dai *data subject*. Riemergeva un rapporto giuridico da utilizzare per imporre degli obblighi a tutela dell'individuo. E gli obblighi conseguenti erano obblighi simili a quelli del "confidente".

La *hard privacy*, dunque, sarà differente dalla *data protection*. La prima ha carattere assoluto (*erga omnes*); la seconda ha carattere relativo (rapporto giuridico tra *data subject* e *data holder*). La prima riguarderà contesti privati, la seconda l'identità contestuale, ossia l'identità personale e l'integrità contestuale. La violazione di domicilio e le interferenze illecite nella vita altrui sono esempi classici di reati relativi alla *hard privacy* (presenti in tutti i Paesi considerati), coniati quando la *data protection* era ancora di là da venire e, soprattutto, poggianti su presupposti giuridici che nulla hanno a che vedere con il trattamento di dati personali. Queste regole sono finalizzate alla tutela di un valore diverso.

Individuato il valore della privacy come identità contestuale (*soft privacy*), potremo quindi analizzare le regole poste dalla *data protection* in una nuova luce. Il punto di equilibrio, sin dal primo atto legislativo statuale in materia (il Data Act svedese del 1973), si rinviene nella tutela del contesto in cui avviene lo scambio di informazioni: esprimendoci in termini molto sintetici, si tratta degli obblighi di trasparenza (preventiva e successiva) del detentore dei dati e del dovere di

[92] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 173 e ss.; Eugene Volokh, cit., p. 1058 e ss.

confidenzialità (principio di finalità - divieto di uso secondario; dovere di impedire accessi non autorizzati). La base legale del trattamento sarà, in ambito privato, il consenso; in ambito pubblico, la legge. Tale ultimo aspetto è certamente quello più tormentato in materia di *data protection* poiché le eccezioni alla regola del consenso si fanno sempre più numerose.

Nel perimetrare il divieto di uso secondario dobbiamo aggiungere al principio di finalità quello di necessità: il *data holder* può raccogliere ed utilizzare solo i dati necessari per raggiungere una determinata finalità. Possiamo, sintetizzando, affermare che la *data protection* pone un generale obbligo di limitazione in capo al *data holder* in base alla finalità del trattamento e alla necessarietà dei dati raccolti rispetto a detta finalità. In tal modo abbiamo perimetrato il contesto entro cui avviene la cessione dei dati dal *data subject* al *data holder*. Obbligo di trasparenza e dovere di confidenzialità in relazione ad un certo contesto delimitato da finalità e necessarietà del trattamento rappresentano ancora oggi il Global Privacy Standard.

In materia di *data protection* l'identità contestuale è il valore tutelato, dunque, ed il tipo di tutela è procedurale: è molto significativo che nella tradizione statunitense si parli piuttosto di *Fair Information Practices*, termine più pregnante dato che rende subito palese che si tratta di pratiche di corretta informazione. Al di là dei valori proclamati dalla tradizione europea, infatti, la sostanza della normativa che consente all'individuo di autodeterminarsi nella sfera sociale si sostanzia in vincoli procedurali all'agire del *data holder*. Non è tanto il diritto dell'interessato quanto il dovere del titolare a risaltare; può altrimenti dirsi, in termini più accurati, che il modello di regolazione non si basa sul diritto assoluto di un individuo

esercitabile *erga omnes* ma è funzione della cornice del rapporto tra individuo e detentore dei dati[93].

È possibile trovare conferma di quanto stiamo dicendo anche facendo ricorso alla miglior dottrina statunitense, utilizzando la norma di appropriatezza di Helen Nissenbaum[94]. Facendo un passo indietro, infatti, notiamo che la *data protection* fa emergere il diritto alla tutela di questa identità (o insieme di informazioni personali) contestuale (ossia legata a un particolare contesto); le violazioni della *data protection* saranno decontestualizzazioni di quell'identità; abbiamo già anticipato, infatti, che il concetto di privacy come identità contestuale collega il concetto di privacy a quello di identità e quello di identità al contesto, riconoscendo una pluralità di contesti differenti (li abbiamo definiti sociali), non solo privati e pubblici. All'interno di ciascun contesto l'archiviazione e la circolazione dei dati avviene in base ad un principio di appropriatezza relativo al tipo e alla quantità di informazioni da trasmettere[95].

Possiamo fare degli esempi: una compagnia area dovrebbe conoscere la città di destinazione del mio viaggio ma non chi incontrerò; un medico dovrebbe conoscere nel dettaglio la mia condizione fisica, il direttore della mia banca no; chiedere delle opinioni politiche ad uno studente in un'aula potrebbe essere inappropriato, salvo casi particolari[96]. Proprio dove questa norma di appropriatezza non è ancora socialmente condivisa, ad esempio nell'uso

---

[93] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 126.

[94] Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 119 e ss.

[95] Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 138.

[96] Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 121.

dei social network, possono sorgere dei problemi. Anche in questo caso si tratta di problemi legati alla contestualità della nostra identità (ciò che abbiamo fatto a vent'anni può non essere più appropriato a quaranta), contestualità che risulta evanescente su Internet, dove i dati sono, da un lato, facilmente accessibili e non proteggibili e, dall'altro, si accumulano e non si cancellano. Ricostruire anche in ambito digitale dei contesti separati e delle identità parziali può essere una soluzione a questo problema. Le principali ragioni per ritenere la contestualità il principio fondamentale è che, fuori contesto, informazioni negative possono diventare umiliazioni permamenti in base ad iniziative poco trasparenti (diffondere informazioni per danneggiare qualcuno) e a giudizi parziali (diffondere solo una parte delle informazioni per influenzare le valutazioni)[97].

Così come esiste una norma di appropriatezza generalmente condivisa tra *data subject* e *data holder*, Helen Nissenbaum individua anche norme di distribuzione delle informazioni tra *data holder*. Sono norme di distribuzione, ad esempio, quelle che regolano i casi e i modi che rendono possibile trasmettere le informazioni sui tabulati telefonici di una persona.

Di fatto il *focus* della normativa sulla protezione dei dati personali riguarda la definizione di norme di appropriatezza e norme di distribuzione[98]. La tradizione del Global Privacy Standard individua in capo al *data holder* un obbligo di trasparenza e un dovere di confidenzialità contestuale. Circoscritto l'ambito della *hard privacy* (informazioni sulla vita privata, sulla vita

[97] Daniel Solove, *No privacy*, cit., p. 97 e ss.
[98] Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 123.

familiare, sulle attività che si svolgono all'interno dell'abitazione, sul contenuto delle nostre comunicazioni), ci troviamo di fronte ad un concetto di *soft privacy*, come tutela della nostra identità (insieme di informazioni personali) in un determinato contesto, presidiato da un obbligo di trasparenza e un dovere di confidenzialità del *data holder*. Così definito, il concetto di *data protection* diviene più preciso e meno vago dell'espressione "diritto alla privacy": si tratta di un primo livello di protezione legato ad un rapporto giuridico tra *data holder* e *data subject*.

Più che a norme di appropriatezza e distribuzione o all'istituto giuridico della confidenzialità, nella normativa europea sulla *data protection* si legge, come si è già anticipato, di un obbligo di trasparenza preventiva e successiva. Tuttavia possiamo provare ad integrare queste concezioni. Preventiva perché occorre che il *data subject* conosca senza dubbio alcuno la norma di appropriatezza (e di distribuzione) vigente in quel contesto; successiva perché al *data subject* è riconosciuto il diritto ad accedere alla sua "ombra" informativa, ossia alla sua identità digitale. Il dovere di confidenzialità impone semplicemente che il *data holder* rispetti la norma di appropriatezza e distribuzione di quel contesto.

Un'ulteriore differenza tra *hard privacy* e *soft privacy*, allora, è che quest'ultima rifugge da prescrizioni universali. Ciò che conta veramente è analizzare come l'introduzione di una nuova pratica o di una nuova tecnologia impatti su di un certo contesto e quindi sulle norme sociali di adeguatezza e distribuzione precedenti.

4. Privacy e Internet: *privacy as new contextual identity*

Nel Global Privacy Standard il centro della

regolamentazione non è più la delimitazione dello spazio privato, caratterizzato dalla inaccessibilità o indisponibilità da parte del potere pubblico (statuale e collettivo) e da precise eccezioni in presenza di un prevalente interesse pubblico, bensì è l'insieme delle nostre informazioni personali (l'identità personale), in particolare sotto il profilo che attiene alla loro archiviazione e circolazione. Siamo al cuore di quello che potremo definire diritto dell'informatica in senso stretto, ossia del diritto dei dati trattati in modo automatico.

Sino ad oggi, tale diritto ha posto due problemi giuridici fondamentali: un problema di proprietà intellettuale e un problema di *data protection*. In entrambi i casi è stato necessario abbandonare un modello proprietario di tutela in favore di nuovi sistemi di protezione. In particolare proveremo a fare anche un *excursus* sulla proprietà intellettuale al tempo della Rete.

Le nuove tecnologie costituiscono certamente un terreno scivoloso per questi valori[99]; per tale ragione è necessario fornire alcune nozioni di base che consentano la comprensione del fenomeno. Anzitutto è necessario chiarire cosa si intenda per dato informatico e per informazione, i due concetti principali intorno ai quali ruota la disciplina in esame. Il dato informatico è una rappresentazione di fatti (o di concetti) in una forma trattata da un sistema di informazione. Informazione, invece, etimologicamente significa "messa in forma"; al

[99] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 47; Guido Rossi, *Il gioco delle regole*, Milano, 2006, p. 62.

suo interno, distinguiamo la struttura dal contenuto[100]. Mentre l'informazione-struttura mette in forma, appunto, un livello di organizzazione, l'informazione-contenuto, detta anche informazione circolante, attiene a tutto ciò che proviene dall'ambiente ed è caratterizzata, pertanto, dall'aleatorietà. Oggi la diffusione dei dispositivi informatici ha incrementato l'informazione-struttura esistente poiché è maggiore la capacità di memorizzare, organizzare e utilizzare l'informazione circolante: le informazioni-contenuto sono presenti e disseminate nella rete Internet su milioni di *server*. Come è noto, in una rete di computer il termine *server* indica genericamente un componente informatico che fornisce, a livello logico e a livello fisico, un qualunque tipo di servizio ad altre componenti che sono chiamate *client*[101]. Le informazioni vengono trasmesse tra un componente informatico ed un altro una volta che sono digitalizzate (la digitalizzazione è il processo di conversione da valori continui a valori discreti) e commutate in pacchetti (il cosiddetto *packet switching*); il *web browser* "traduce" queste informazioni digitali in testi, foto e video, quindi le informazioni si trovano su un *server*. Le informazioni, grazie ai protocolli,

[100] Henry Laborit, *La vita anteriore*, Mondadori, Milano, 1990, p. 109 e ss.

[101] Se ci fossero un solo *server* ed una molteplicità di *client*, sarebbe estremamente facile comprendere dove fisicamente si trovano le informazioni in rete. Così, però, non è: i *server*, come detto, sono milioni. Per questo abbiamo bisogno di un "indirizzo" che ci consenta di arrivare a quelle informazioni che ci servono presenti su quei *server* che non conosciamo. Il *world wide web* (il WWW) è un sistema di *server* Internet che supportano i documenti formattati in un determinato linguaggio (quello più diffuso è l'HTML) che supporta i collegamenti tra risorse (i *link*). Sul *world vide web*, il *web address* è chiamato anche URL.

possono essere visualizzate sul nostro computer attraverso un *web browser* che traduce in parole, immagini, video le sequenze digitali in cui le informazioni sono scomposte.

Nell'era dell'informazione web 2.0 e dei social network, è difficile sottrarsi ai nuovi media o semplicemente controllarli: la semplicità con cui si copiano e si diffondo le informazioni è sbalorditiva. Si pensi al cosiddetto *Barbra Streisand Effect*: nel 2003 la celebre cantante provò a far rimuovere la foto della sua villa in California con un'azione giudiziaria per violazione della privacy. Il sito accusato della violazione, che prima dell'azione poteva contare su pochi accessi, ricevette in pochi giorni 420.000 visite.

Le tecnologie dell'informazione hanno un ruolo essenziale e inconfondibile: la capacità di memorizzazione dei dati e la potenza di elaborazione (informazione-struttura) hanno permesso livelli inimmaginabili di aggregazione e analisi di una enorme quantità di dati personali (informazione-contenuto). La sempre maggiore facilità di raccolta e analisi delle informazioni personali ha posto l'esigenza di tutelare la nostra identità personale, ossia la nostra autonomia nella determinazione delle informazioni che circolano sul nostro conto. Quello che proponiamo è di tutelare la nostra identità contestuale, ovvero l'insieme delle informazioni che ci riguardano e che sono collegate ad uno specifico contesto in cui è avvenuto uno scambio di informazioni.

Da valore colto in negativo (libertà da), la privacy ha mutato pelle diventando una pretesa di controllo sulle proprie informazioni, quindi sulla propria identità. Controllo che però appare impossibile. Non si tratta di sottrarsi dalla sfera pubblica, quanto piuttosto di muoversi all'interno di essa.

Di fatto è una sorta di pretesa di privacy in pubblico,

per usare l'espressione di Helen Nissenbaum[102]. Tuttavia il punto è non tanto controllare i nostri dati, quanto piuttosto conoscere i contesti nei quali ci muoviamo e pretendere che le informazioni che ci riguardano non vengano decontestualizzate. Intendiamoci: abbiamo chiarito che in alcuni casi (intercettazioni, trasparenza dell'azione della pubblica amministrazione) la soluzione deve passare attraverso le norme elaborate con riferimento alla privacy in senso negativo. In molti casi, tuttavia, il tema è diverso e passa attraverso la cosiddetta *data protection*, ossia la regolazione dell'identità contestuale.

Riassumendo: occorre abbandonare la dicotomia privato e pubblico perché questa si basa sui concetti di accessibilità e disponibilità che divengono sempre più sfuggenti. La protezione dei dati personali viene garantita a prescindere dalla considerazione del carattere privato o pubblico dell'informazione. L'informazione è personale ed in quanto tale trova tutela all'interno della relazione tra *data subject* e *data holder*.

Dopo la *tort privacy* (divulgazione di dati privati quale minaccia alla tranquillità) e la *constitutional privacy* (intromissione nella sfera di libertà dell'individuo), possiamo parlare dell'*informational* o *data base privacy*, generalmente nota come disciplina sulla protezione dei dati personali o *data protection*, nella consapevolezza dei vari valori che più o meno direttamente vengono in rilievo. Per la *data protection*, si tratta della normativa relativa all'archiviazione e alla circolazione delle informazioni personali. Il centro della regolamentazione non è più la

[102] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, in *Law & Philospophy*, 1998, p. 559.

delimitazione dello spazio privato inaccessibile o accessibile solo nel rispetto di precise garanzie giuridiche ma l'insieme delle nostre informazioni personali (l'identità) e la loro archiviazione e circolazione. Il controllo della nostra identità, soprattutto se consideriamo l'identità digitale - sempre più accessibile, sempre più ricca e sfaccettata -, diventa assai sfuggente se non tecnicamente ed economicamente impossibile.

Occorre delimitare i contesti e stabilire le regole che i *data holder* devono rispettare.

Nel 2010, gli utenti della Rete nel mondo erano quasi 2 miliardi, poco meno di un terzo della popolazione mondiale; 600 milioni i profili presenti sul principale social network (con 30 miliardi di contenuti - post, foto e video - condivisi ogni mese); 175 milioni i profili attivi sul più importante sito di *micro blogging*; quasi 100 milioni i siti con domini .com su 255 milioni di siti registrati; 35 ore di video caricati ogni ora sulla più nota piattaforma di *video sharing*; 5 miliardi di foto memorizzate sul più diffuso servizio di *hosting*; 1,6 miliardi i cellulari venduti, di cui circa 300.000 smartphones. Le nuove tecnologie informatiche consentono non solo di rendere disponibile al pubblico ma anche di registrare una mole impressionante di informazioni: il *data subject* condivide queste informazioni sia volontariamente che involontariamente.

A questo riguardo, abbiamo sia trattamenti di informazioni in cui è l'utente a trasmettere i propri dati personali al fornitore del servizio, sia trattamenti in cui è il fornitore di servizi a rilevare dati personali dell'utente. Quanto ai trattamenti volontari, si prenda il fenomeno del *life* o *self tracking*, esemplificato da Matteo Bittanti, ricercatore sui nuovi media all'Università di Stanford, che scrive in "Homo Sapiens 2.0 – la mia vita in cifre": "Faccio jogging in media tre volte alla settimana. Per lo

più il giovedì. Percorro almeno 41 chilometri. Nell'aprile del 2010 – miglior performance in assoluto – ho totalizzato 169 chilometri. A dodici mesi di distanza voglio sfondare il tetto dei 200. Secondo Nikeplus.com, ho il 73% di possibilità di raggiungere questo obiettivo, obiettivo che ho comunicato ai miei fans, followers e friends. Nel 2010 ho bruciato 76.972 calorie. Oggi ho camminato per 5,2 chilometri, pari a 10.353 passi. Consumo in media 11 cappuccini doppi con latte scremato alla settimana che mi forniscono (caduno) 90 calorie, 4,5 grammi di grassi, 5 grammi di proteine e il 15% del fabbisogno giornaliero di calcio. Tra il 15 e il 21 marzo 2011 ho consumato 10.643 calorie, 308 grammi di grassi, 500 milligrammi di colesterolo, 7.746 grammi di sodio, 1.071 carboidrati, 132 grammi di proteine, 403 grammi di proteine e 367 di zuccheri". Come afferma Zygmunt Bauman[103], non si può più ritenere che il pubblico colonizzi il privato, quanto piuttosto il contrario: è il privato che oggi va colonizzando lo spazio pubblico, ridotto allo schermo di un computer, spazzando via tutto quanto non possa essere pienamente espresso nel gergo dei fini, degli interessi e dei timori privati. Fenomeno esploso con il web 2.0 e con i social network, che sarà ulteriormente esaltato dalla diffusione dei servizi di *cloud computing* e dal conseguente trasferimento di spazi "privati", per definizione non generalmente accessibili, in luoghi sottratti alla piena disponibilità del singolo (servizi di *hard disk* remoto, *web mail* e *web calendar*, *software* di scrittura e di calcolo).

Non basta: quanto ai trattamenti involontari, si prenda in considerazione il tema dei *cookies*, piccoli *files* di testo inviati da un *server* e registrati da un *client*, di

[103] Zygmunt Bauman, cit., p. 20.

solito il programma di navigazione o *browser* degli utenti, per consentirne e facilitarne l'uso (il *client* ri-trasmette il *cookie* al server a ogni accesso consentendone il riconoscimento e l'identificazione). I *cookies* danno la possibilità di raccogliere informazioni sull'utente o quanto meno sul dispositivo da lui utilizzato: l'indirizzo IP, il *browser*, il sistema operativo, data ed ora di navigazione, il tempo di permanenza etc. E il tema è: deve essere considerato un trattamento tra un *provider* di servizi ed un utente oppure tra due sistemi telematici? Un problema di libertà (in senso negativo, quindi di controllo e sorveglianza) o un problema di funzionalità? Oppure si prenda in considerazione il tema, collegato a quello dei *cookies*, della *Web Analytics*, ossia della raccolta, misurazione ed analisi dei dati di traffico su un sito Internet a fini di comprensione e di ottimizzazione dell'utilizzo del web. Saranno i *cookies* a determinare la possibilità di conteggiare i visitatori unici di un certo sito e l'attività che quell'utente fa. Il rifiuto dei *cookies* o la loro successiva cancellazione porta a errore di raccolta, misurazione ed analisi dei dati di traffico di un sito. Anche in questo caso, è un problema di libertà o di funzionalità? Analogo è il problema della profilazione, ossia della tecnica che permette di dedurre informazioni e compiere previsioni di comportamento relative a un individuo sulla base di tutti i dati relativi ad un gruppo cui quell'individuo appartiene. È chiaro che esiste una profilazione "buona" che consente all'interessato di ottenere dei servizi basati sui suoi comportamenti precedenti e una profilazione "cattiva" che può portare scelte discriminatorie da parte del soggetto erogatore del servizio. Dal punto di vista tecnico, la profilazione è spesso utilizzata durante la navigazione in Internet o nell'utilizzo di applicazioni per smartphone. Le nuove tecnologie consentono di

memorizzare enormi quantitativi di dati e di procedere molto rapidamente a elaborare automaticamente decisioni e valutazioni. Tanto più se la profilazione viene abbinata, ad esempio, a servizi di geolocalizzazione in modo da prevedere le preferenze del consumatore e offrire servizi estremamente personalizzati.

Queste ipotesi non devono essere sempre considerate come questioni di libertà negativa, almeno sotto il profilo del modello di tutela.

Internet (informazione-struttura) ha incrementato la circolazione in tempo reale di quantità inimmaginabili di dati (informazione-contenuto): è l'era delle informazioni trattate in modo automatico, è l'era informatica; tra le altre, circolano come mai in precedenza informazioni protette dal diritto d'autore e informazioni personali.

Come abbiamo già accennato, sotto quest'ultimo profilo l'informazione-contenuto in un contesto informatico non solo circola in tempo reale da un luogo all'altro del globo ma è archiviata in maniera persistente nel tempo. Ciò crea il forte rischio che esse siano raccolte in un determinato contesto e siano invece utilizzate fuori contesto sincronicamente o diacronicamente. Una foto personale caricata su un social network, magari non troppo decorosa, può essere utilizzata da un potenziale datore di lavoro oggi e da un potenziale partner tra dieci anni. La conseguenza, qualora tale rischio si avverasse, sarebbe una violazione della privacy in senso positivo, ossia dell'identità personale contestuale, violazione che dobbiamo sempre considerare sia in senso sincronico sia in senso diacronico, comportando lo scontro frontale con l'autonomia informativa, appunto la privacy positiva. Si prenda il caso, ancora, di un pettegolezzo relativo ad una mancanza di una persona circolato in un determinato ambiente (ad esempio, in un contesto universitario e

riferito ad uno studente o a un professore) che, se pubblicato su un blog, resta visibile per anni e quindi diviene conoscibile in un ambito diverso (ad esempio in ambito lavorativo). Il rischio maggiore è che una piccola mancanza, quindi un'informazione negativa particolare, costituisca la base per un giudizio generale d'inaffidabilità di una persona. Oppure, sincronicamente, che le valutazioni di un professore su quello studente e dello studente su quel professore non attinenti al contesto di formazione e studio, possano determinare dei pregiudizi per l'uno o per l'altro[104].

La digitalizzazione ha messo in crisi – più che la tradizionale contrapposizione tra privato e pubblico – la nozione d'identità, in quanto concetto dipendente dal contesto e dal tempo. Oggi, infatti, è diventato possibile memorizzare e raccogliere molti attributi riferibili a un soggetto collegando tra loro le varie identità parziali, creando una iper-identità. Il contesto informatico, il contesto delle informazioni trattate in modo automatico, rende possibile aggregare le identità parziali dell'individuo sia sincronicamente (tutte le informazioni presenti in un dato momento) sia diacronicamente (tutte le informazioni presenti nel tempo). A tal proposito, parliamo frequentemente d'identità digitale perché spesso le informazioni riferibili a una persona sono memorizzate su supporti informatici.

In tal senso, anche l'anonimato, gli pseudonimi, le diverse credenziali di autenticazione, i profili di autorizzazione diventano strumenti fondamentali per la gestione della nostra identità. Alle identità parziali rischia

[104] Casi realmente accaduti: Daniel Solove, *No privacy*, cit., p. 68 e ss.

di sostituirsi l'iper-identità, realizzando la metafora dell'individuo trasparente[105] (o quella più nota della società trasparente di David Brin[106]), perennemente e totalmente esposto allo sguardo e al giudizio altrui. Anche in questo caso tenere distinta la privacy-intimità (negativa) dalla privacy-identità (positiva) vuol dire comprendere meglio le diverse discipline che su questi valori si basano. La tecnologia, in realtà, non impatta solo sull'identità, slegandola dal contesto e dal tempo, ma modifica radicalmente il concetto stesso di sfera pubblica sino a renderlo evanescente, fino a che il confine tra privato a pubblico tende a svanire; ciò era già accaduto ai tempi di Warren e Brandeis ed è cronaca quotidiana nella società trasparente dominata da Internet e dall'IT[107].

Le tecnologie, e ciò è fuor di dubbio, limitano fortemente la possibilità dell'individuo di sottrarsi dalla sfera pubblica (privacy-intimità) o di autodeterminarsi nella sfera pubblica (privacy-identità). È importante notare, infatti, che il punto di equilibrio tra interessi contrapposti viene costantemente spostato in avanti (a svantaggio della riservatezza, evidentemente) dalla diffusione di nuove tecnologie, quali (a titolo esemplificativo ma non esaustivo) i *social media*, il *cloud computing*, la geolocalizzazione nonché tutti gli strumenti atti ad intercettare flussi informatici o telematici.

Riepilogando, dunque, abbiamo preso le mosse dalla privacy come valore, riconoscendo due diversi aspetti che abbiamo sintetizzato nelle espressioni privacy-intimità e privacy-identità. La prima trova nella pretesa di agire

[105] Stefano Rodotà, *La vita e le regole*, cit., p. 104.
[106] In un mondo in cui tu sai tutto di me, io so tutto di te.
[107] Lisa Austin, cit., p. 120.

indisturbati e quindi in una serie di garanzie poste da norme costituzionali, penali e civili la propria proiezione giuridica; la seconda, invece, si concreta in una serie di obblighi che incombono sul *data holder* e che dovrebbero dare contenuto alla pretesa dell'interessato di esercitare un controllo sulla possibilità di raccogliere, archiviare e far circolare informazioni personali.

Come si è già avuto modo di rilevare in precedenza, il diritto alla privacy nasce negli U.S.A. alla fine del diciannovesimo secolo; in tali coordinate spazio-temporali, il contenuto del diritto alla privacy si sintetizzava in tre comandi: 1) impedire che fatti privati venissero divulgati pubblicamente o comunque ponessero in cattiva luce un determinato soggetto (e, in caso di divulgazione, obbligare al risarcimento del danno); 2) impedire che l'immagine di un individuo che non rivestisse un ruolo pubblico venisse usata senza il suo consenso (e, in caso di indebita utilizzazione, obbligare al risarcimento del danno); 3) impedire che l'Autorità prendesse cognizione di fatti privati. Appare da subito evidente come il concetto di privacy come diritto si colleghi, da questo angolo visuale, al concetto di privacy come valore, nella sua accezione di libertà negativa (cioè quella che abbiamo chiamato privacy intimità).

La regolamentazione della protezione dei dati personali, invece, nasce a partire dagli anni '70 del secolo scorso: i primi provvedimenti in materia di protezione dei dati personali, come visto, si devono a Germania (in due *Länder* tedeschi nel 1970), Svezia (1973) e Stati Uniti (1974). In origine, il contenuto del diritto alla protezione dei dati personali era duplice: in primo luogo, evitare che l'Autorità creasse database segreti; in secondo luogo, impedire l'uso "secondario" di questi database, ossia l'uso ulteriore rispetto a quello consentito dall'ordinamento: ad

esempio, in caso di raccolta dati in occasione di un censimento, i quali evidentemente non possono essere adibiti ad utilizzo diverso da quello della mappatura sociale, scopo per cui sono stati richiesti e forniti.

La questione, almeno all'inizio, era (allora) e resta (ora) quella di limitare l'ingerenza del potere pubblico nella vita privata degli individui; ma occorre sottolineare che ci sono almeno due differenze fondamentali rispetto al momento storico in cui il problema è sorto: anzitutto il cuore della disciplina non è più la distinzione tra contesto privato e contesto pubblico, in quanto oggetto della regolamentazione è il dato personale (concetto che non coincide esattamente con quello di dato privato); se è vero, poi, che bisogna essenzialmente limitare l'esistenza di database segreti, il problema principale diventa la regolamentazione della condivisione e circolazione di questi dati, ossia quello che abbiamo definito *data sharing*. In siffatto quadro, il *focus* della disciplina non è tanto il diritto in capo all'interessato (*data subject*) quanto gli obblighi gravanti sul detentore dei dati (*data holder*). Da quest'altro angolo visuale, invece, il concetto di protezione dei dati personali si collega al concetto di privacy come valore, nella sua accezione di libertà positiva (privacy-identità).

L'uso dell'espressione "diritto alla privacy" per riferirsi alla proiezione giuridica di ambedue questi valori provoca confusione nella ricostruzione dei modelli di tutela: proprio a partire dagli anni '60 e '70 il contenuto del diritto alla privacy (quella il cui valore sotteso è la privacy-intimità) ha finito per sovrapporsi al contenuto del diritto alla protezione dei dati personali (il cui valore sotteso è, invece, la privacy-identità).

Il Global Privacy Standard affonda le proprie radici nella citata legislazione degli anni settanta e nelle

convenzioni internazionali degli anni ottanta del secolo scorso, e di questa ambiguità (privacy-intimità e privacy-identità) porta le tracce. Anzitutto, è necessario chiarire che l'ambito di applicazione del Global Privacy Standard non riguarda la cosiddetta *spatial privacy*, non ci si preoccupa, cioè, di delimitare lo spazio privato per proteggerlo dall'intrusione di quello pubblico, nemmeno quando l'attenzione si concentra sulle comunicazioni, ossia uno degli ambiti tradizionalmente associati alla *hard privacy*, ma si delineano, come anticipato, gli obblighi del *data holder* per quanto concerne la creazione, la gestione e l'utilizzo delle banche dati, preoccupandosi, perciò, dei dati personali contenuti negli archivi elettronici e non anche dei fatti privati. Restando all'esempio delle comunicazioni, il contenuto di tali comunicazioni rientra nel modello di tutela della *privacy as dignity* mentre la *data protection* garantisce un primo livello di protezione di tutti i dati esteriori di queste comunicazioni (quando, come, per quanto tempo). Il *data holder* ha un primo obbligo di confidenzialità nella gestione di questi dati. Che tra i due concetti, *privacy as intimacy* e *privacy as identity*, esista una parziale sovrapposizione[108] (che giustifica l'uso frequente di tali termini quali sinonimi) non può essere messo in dubbio; basta, però, mettere a confronto quanto sin qui detto sulla contrapposizione tra il contenuto del diritto alla privacy e quello del diritto alla protezione dei dati personali per svelare una chiara distinzione: se il primo si concreta essenzialmente nell'impedire che fatti privati vengano divulgati pubblicamente, nel secondo ciò che viene in evidenza è il – presunto – potere di controllare l'uso dei propri dati personali attraverso l'imposizione di

[108] Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 485.

obblighi sul gestore della banca dati. Da ciò risulta lampante la distinzione tra i due aspetti sia sotto il profilo del contenuto del diritto (impedire *versus* controllare), sia sotto il profilo dell'oggetto del diritto (fatti privati *versus* dati personali).

Come ampiamente argomentato, la *ratio* sottesa al diritto alla protezione dei dati personali e, dunque, al rapporto tra *data subject* e *data holder* è essenzialmente quella di porre strumenti a tutela della libertà positiva di autodeterminazione della propria identità personale ("libero di"). Un valore ben diverso, lo si ripete, è quello protetto dal diritto alla privacy tradizionale, cioè la propria libertà d'azione (ossia la libertà di agire senza ingerenze esterne, "libero da").

Per fare ordine, quindi, occorre chiarire che il diritto alla privacy esprime anzitutto la "libertà da" qualcosa (in senso negativo), una sorta di possibilità di agire e scegliere al di fuori della dimensione pubblica e al riparo da intrusioni (l'abbiamo definita *hard privacy* – nocciolo duro della libertà individuale riconosciuta dall'ordinamento); mentre il diritto alla protezione dei dati personali è strumento di tutela della privacy valore in senso positivo, poiché si manifesta quale "libertà di" determinare come la propria identità personale si sviluppa nella dimensione pubblica (l'abbiamo definita *soft privacy* – possibilità di plasmare le nostre identità parziali). Due modelli di tutela differenti: uno strumento di opacità il primo (si tutela l'interesse a celare comportamenti e scelte), uno strumento di trasparenza il secondo (si tutela l'interesse del *data holder* a trattare i dati ma in modo leale e corretto).

Storicamente il primo diritto emerge settant'anni prima del secondo; quando li si analizza insieme raramente si mette in evidenza che i valori sottesi sono ben differenti e non solo, come visto, per la loro data di nascita. Ciò

finisce per rendere vaghi anche i contenuti giuridici che da quei valori traggono origine. Il diritto traduce, invece, valori ben precisi: da un lato libertà e autonomia dalla dimensione pubblica; dall'altro libertà e autonomia (o, forse in maniera più pregnante, identità) nella dimensione pubblica. Il Global Privacy Standard riguarda essenzialmente quest'ultima dimensione giuridica; mentre, invece, norme di rilievo costituzionale e penale tutelano la prima dimensione del diritto alla privacy, quale estrinsecazione di una libertà negativa. Riferirsi, come abitualmente si fa, alla privacy sia come diritto di impedire la divulgazione di fatti privati sia come diritto di controllare la circolazione dei propri dati personali rischia solo di confondere.

Nel garantire tutela ai beni che s'intende proteggere, infatti, non può certo prescindersi dalla loro puntuale declinazione. Come si vedrà, le regole a tutela del diritto alla privacy (nel senso di privacy-intimità) si differenziano da quelle a tutela del diritto alla protezione dei dati personali (privacy come identità); basti pensare a quanto la privacy sia fortemente legata al contesto sociale e politico di un determinato momento storico.

5. Privacy e proprietà intellettuale: *privacy as copyright*

Il contesto digitale che abbiamo descritto coinvolge sia la circolazione di dati personali sia di contenuti protetti dal diritto d'autore. Descritto il problema della privacy come controllo sui propri dati personali, emerge un chiaro parallelismo con il tema della tutela del copyright (controllo dei dati su cui posso vantare una serie di diritti, morali ed economici). Secondo questa prospettiva l'opera su cui vantare tali diritti sarebbe la nostra identità.

Un parallelo che fa perno sul concetto di proprietà e sulla sua estrema malleabilità: esso può riguardare sia la cosiddetta proprietà intellettuale sia i dati personali che costituiscono la nostra identità contenstuale, regolandone quindi distribuzione, riproduzione e circolazione.

Eppure proprio la diffusione di Internet ha comportato sia una ridefinizione della *data protection* e del diritto alla privacy sia un ripensamento della proprietà intellettuale: proprio per il copyright il modello proprietario si è dimostrato scarsamente efficace.

L'uso dei sistemi *peer-to-peer* (P2P) d'altronde costituisce una "vera e propria sfida alle leggi sul copyright e, più in concreto, alla possibilità del loro *enforcement*"[109]. La normativa sul *copyright* si basa sul presupposto che le opere protette siano copiabili con difficoltà e che la loro copia sia pur sempre inferiore rispetto all'originale dal punto di vista qualitativo. Oggi, al contrario, il *file sharing* consente di ottenere facilmente copie perfette. Grazie al P2P, infatti, "gli utenti Internet possono condividere in rete file di vario genere, sostanzialmente mettendo a disposizione di tutti coloro che sono collegati al sistema e possiedono i necessari requisiti di sistema le opere dell'ingegno contenute nei file in questione"[110]. Le barriere di accesso a un sistema di *file sharing* sono di fatto inesistenti: chiunque può accedervi,

---

[109] Ovverosia della loro attuazione coercitiva; Giovanni Pascuzzi, *Il diritto dell'era digitale*, Bologna, Il Mulino, 2002, p. 149.

[110] Simona Lavagnini, *La proprietà intellettuale in Internet*, in *AIDA Annali italiani del diritto d'autore, della cultura e dello spettacolo,* 2005, p. 277; *"la condivisione di file tramite reti "peer-to-peer" è una delle più efficienti fra le già efficienti tecnologie attivate dalla rete"* Lawrence Lessig, *Cultura libera*, Milano, Apogeo, 2005, p. 17.

copiare abusivamente opere digitali protette dal diritto d'autore e metterle a disposizione di altri utenti. Pertanto un sistema del genere consente con estrema facilità, a bassissimo costo, senza intermediari e a livello globale di condividere contenuti digitali (illegali o meno) di qualsiasi tipo. Tradizionalmente il mercato più esposto a questo fenomeno è stato quello musicale, anche se oggi assistiamo a un forte incremento degli scambi di video (film) e software; più in generale aumenta in modo esponenziale la diffusione di contenuti digitali del tutto immateriali e per conseguenza s'impone un profondo ripensamento del regime di appropriazione legato a tali beni.

Se il copyright basato sul concetto di proprietà è messo in discussione dal contesto digitale nel quale viviamo, analogamente dovremmo analizzare criticamente una descrizione della privacy in termini di copyright. In entrambi i casi è il modello proprietario di tutela che non sembra idoneo a raggiungere lo scopo di tutela che si prefigge. Il modello di tutela sottostante alla proprietà intellettuale è, come dice la parola stessa, il diritto di proprietà. In maniera del tutto analoga, come abbiamo visto, il modello a tutela del *right to privacy* di Warren e Brandeis era sempre il diritto di proprietà. Nell'uno e nell'altro caso tale riferimento alla proprietà risulta insufficiente e fuorviante.

Si pensi, in materia di copyright, al parallelismo tra furto e violazione del diritto d'autore: il furto di un libro dagli scaffali di una libreria implica il fatto che ci sarà una copia in meno da vendere (impossessamento e sottrazione); scaricarlo abusivamente (impossessamento) e diffonderlo in rete tramite P2P moltiplicherà il numero di esemplari senza comportare alcuna sottrazione.

In materia di privacy, invece, abbiamo visto che la tutela accordata attarverso la disciplina della *privacy as dignity* (intercettazioni, tutela rispetto alla diffusione di fatti privati) e della *data protection* (diritto alla propria identità personale e contestuale, attraverso obblighi di confidenzialità imposti su chi tratta i dati) risulta inspiegabile attraverso le lenti del paradigma proprietario perché altri sono i valori sottostanti.

Tuttavia si deve a Zittrain il parallelismo, cui abbiamo fatto cenno, tra privacy, copyright e modello proprietario di tutela: in entrambi i casi si tratterebbe di "*control over data*". Eppure la pretesa di tutelare in maniera assoluta i diritti di proprietà intellettuale "relativamente a beni immateriali diffusi attraverso Internet, rischia di risultare velleitaria e, a volte, nemmeno rispondente ad esigenze di giustizia sostanziale. Si pone, quindi, il problema di ricercare soluzioni efficaci, anche a rischio di affievolire, nel mondo di Internet, la tutela di cui tali diritti godono nel mondo *off line*"[111]. Se dunque non risulta molto utile assimilare privacy e copyright in base al concetto di proprietà sui dati, da un lato dati personali e dall'altro dati protetti dal diritto d'autore, rileviamo una tendenza comune.

I titolari dei diritti di sfruttamento commerciale sulle opere d'arte, infatti, fanno ricorso sempre più spesso ad una sorta di autotutela tecnica introducendo nei loro prodotti misure tecniche (anti-copia o anti-accesso) a protezione delle opere che commercializzano per monitorare l'uso che ne viene fatto ed impedirne usi non autorizzati.

---

[111] Ugo Draetta, *Internet e commercio elettronico*, Milano, Giuffrè, 2005, p. 44.

E' il tema, assai controverso, del DRM: *digital rights management*, che può trovare un immediato parallelismo nelle *Privacy Enhancing Technologies*, o PETs[112], ossia quegli strumenti tecnici che consentono all'individuo di preservare il proprio anonimato o di impedire la diffusione di alcune informazioni oppure ancora di monitorare i dati che vengono scambiati durante la navigazione in Internet.

Proprio con riferimento ai *digital rights management,* Viktor Mayer Schönberger ha proposto di abbinare al dato (sia esso contenuto protetto o dato personale) una metainformazione su chi e come possa usarlo.

Ovviamente il tema delle *Privacy Enhancing Technologies* non si limita a questo strumento ma chiarisce, una volta di più, che in ambito globale gli strumenti tecnologici vengono spesso privilegiati rispetto agli strumenti giuridici.

Così come abbiamo fatto per la privacy, anche per il copyright analizzare le ragioni della tutela vuol dire interrogarsi sui valori sottostanti questa disciplina, su chi sono i soggetti tutelati e su come vengono tutelati.

Lo scopo del sistema del diritto d'autore (e anche di quello brevettuale)[113] consiste nel promuovere le

---

[112] Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 125; Eugene Volokh, cit., p. 1066; Neil M. Richards, *Intellectual privacy*, cit., p. 314; Yang Wang e Alfred Kobsa, *Privacy-Enhancing Technologies*, in AA.VV, *Handbook of Research on Social and Organizational Liabilities in Information Security*, Hershey, IGI Global, 2009, p. 204 e ss.

[113] Brevetto e *copyright* costituiscono due differenti modi di acquisizione del diritto sulle creazioni intellettuali (il brevetto sulle invenzioni, il *copyright* sulle creazioni intellettuali tra cui il *software*) con differenti modalità di acquisizione del diritto (nel

innovazioni garantendo agli inventori e agli autori, oltre ai diritti morali sull'opera, il diritto di sfruttare economicamente per un periodo di tempo limitato le rispettive scoperte o creazioni; in altre parole, il titolare del diritto (di proprietà intellettuale) ha la facoltà di riservare a sé (o, come più spesso accade, cedere a terzi) il potere esclusivo di trarre profitto dalla propria opera.

Il valore della privacy in senso negativo è la tutela di una quota di libertà riconosciuta all'individuo nella società in cui vive e il valore della privacy in senso positivo è la possibilità di decidere come agire all'interno della sfera pubblica, ossia la possibilità di plasmare l'identità del singolo nei vari contesti in cui cede informazioni.

Il modello proprietario rappresenta storicamente un primo modello di tutela sia per il diritto d'autore (copyright) sia per la privacy (*spatial privacy*). Nel contesto digitale, tuttavia, non garantisce, nell'uno e nell'altro caso, risposta certa alle esigenze di tutela.

Approfondendo questo aspetto, può dirsi, ancora che il diritto d'autore si fonda sulla tutela dello sfruttamento commerciale di un'opera dell'ingegno attribuito in esclusiva al suo creatore. Tale sfruttamento si traduce nel diritto di copiare (*copy-right*) e diffondere, in qualsiasi forma, la propria creazione[114]. Per un periodo di tempo

---

primo caso dalla data in cui la domanda di brevetto è resa accessibile al pubblico, nel secondo dalla creazione dell'opera), differente durata del diritto (nel primo caso 20 anni dalla data di deposito della domanda, nel secondo 70 anni dalla morte dell'autore), differenti strumenti giuridici di difesa: Giusella Finocchiaro, *Diritto di Internet*, Bologna, Zanichelli, 2001, p. 153.

[114] Gino Scaccia, *Il bilanciamento degli interessi in materia di proprietà industriale*, in *AIDA*, cit., p. 199; sicchè tale diritto trova fondamento nella tutela del lavoro in ogni sua declinazione (art. 35

stabilito dalla legge la circolazione del bene, in ogni sua possibile forma di utilizzazione, deve essere autorizzata dall'avente diritto: in primo luogo, come detto, dall'autore[115], quindi dai soggetti titolari dei diritti derivati, ossia da quei soggetti cui l'autore abbia ceduto il proprio diritto originario. Fatta eccezione per i casi di libera utilizzazione[116], altri usi senza il consenso del titolare o dei titolari del diritto sono illeciti[117]. Come detto, sia la disciplina dei brevetti sia quella sul diritto d'autore sono modellate sul concetto di proprietà privata su beni materiali. In estrema sintesi: il bene in senso giuridico è ciò che può essere oggetto di un diritto; il diritto è un potere riconosciuto dall'ordinamento per la soddisfazione di un interesse; la proprietà è il diritto (quindi il potere) più ampio di godere e disporre di un determinato bene riconosciuto dall'ordinamento. La proprietà si esercita essenzialmente su beni materiali; il bene tutelato dalla proprietà intellettuale, invece, è immateriale. Tuttavia la

---

Cost.), nella libertà d'impresa (art. 41 Cost.), nella salvaguardia dei diritti fondamentali dell'individuo all'espressione di sé (art. 3 Cost.) e nella promozione della cultura e della ricerca (art. 33 Cost .).

[115] O una molteplicità di soggetti, come avviene, ad esempio, nel caso dell'opera multimediale, Giusella Finocchiaro, cit., p.164.

[116] In base alla dottrina anglosassone del *fair use* talvolta è consentito copiare materiali protetti: "I criteri da prendere in considerazione sono relativi alla natura dell'utilizzo (consentito quello *no profit*, a fini educativi, ma non quello commerciale), alla natura dell'opera, alla quantità copiata (meno è, meglio è) e all'entità del pregiudizio patrimoniale ai danni del legittimo titolare del diritto" David D. Friedman, *L'ordine del diritto*, Bologna, Il Mulino, 2004, p. 124.

[117] Laura Chimienti, *Lineamenti del nuovo diritto d'autore*, Milano, Giuffrè, 2004, p. 405.

giustificazione per questo potere è lo stesso: il lavoro dell'individuo. Quindi, in modo del tutto analogo, sia chi gode della proprietà di un bene materiale sia chi crea un bene immateriale può vantare dei diritti di esclusiva sul bene stesso. Pertanto il titolare ha il potere di escludere[118] dal godimento di quel determinato bene chiunque non sia autorizzato. Il particolare statuto di limitata accessibilità e disponibilità è lo stesso rispetto ai fatti privati o alle informazioni personali ed è per questo che abbiamo messo in luce un possibile parallelismo.

Tuttavia la giustificazione di tale potere di esclusione è del tutto diversa: il valore del diritto d'autore sta nell'incentivare e promuovere la creatività e l'innovazione; il valore della privacy in senso negativo è garantire una quota di libertà rispetto all'invadenza dello Stato e della collettività; in senso positivo la possibilità di scegliere come essere rappresentato nello spazio pubblico.

Il modello di tutela traduce in norme questi valori, contemperandoli con altri interessi che l'ordinamento ritiene rilevanti; per tale ragione rispecchia (o dovrebbe rispecchiare) nella maniera più efficace possibile il valore che intende realizzare.

Di questa dialettica assiologica bisogna tener conto. In materia di copyright, ad esempio, l'esclusiva, cui abbiamo fatto riferimento, non è assoluta: vi sono limiti giuridici e limiti tecnologici. In primo luogo, è evidente il beneficio sociale rappresentato dalla diffusione e dalla libera fruizione delle nuove conoscenze. Sotto questo profilo emerge il diritto a essere inclusi nel godimento del bene-prodotto culturale, poiché sussiste un interesse

[118] Gino Scaccia, *Il bilanciamento degli interessi in materia di proprietà industriale*, in *AIDA*, cit., p. 205.

generale alla libera circolazione e alla diffusione della cultura e allo sfruttamento di ogni creazione. Vi è dunque una tensione tra diritti di esclusiva e diritti di accesso: il diritto a essere inclusi nella rete della cultura (che è un interesse pubblico) che deve coordinarsi con il diritto ad escludere da quella stessa rete salvo il pagamento di un compenso (che è un interesse privato)[119]. Traccia di questa tensione si rinviene anche nella Dichiarazione Universale dei diritti umani, proclamata il 10 dicembre 1948 dall'Assemblea Generale delle Nazioni Unite, che all'art. 27 prevede: 1) che ogni individuo ha diritto di prendere parte liberamente alla vita culturale della comunità, di godere delle arti e di partecipare al progresso scientifico ed ai suoi benefici; 2) che ogni individuo ha diritto alla protezione degli interessi morali e materiali derivanti da ogni produzione scientifica, letteraria e artistica di cui egli sia autore.

Tra i diritti fondamentali dell'uomo si inscrive dunque il diritto del singolo a godere degli interessi morali e materiali scaturenti dalla sua produzione scientifica, letteraria o artistica[120] ma tale diritto deve essere contemperato con l'interesse pubblico alla promozione e alla circolazione della cultura, ovvero con un valore di rango costituzionale.

---

[119] Jeremy Rifkin, *L'era dell'accesso*, Milano, Mondadori, 2000, p. 317.

[120] I diritti morali derivanti dalla creazione di un'opera culturale sono: il diritto di paternità, il diritto di rivelazione, il diritto di pubblicazione, il diritto all'integrità dell'opera, il diritto al suo ritiro. I diritti materiali sono i diritti di sfruttamento dell'opera derivanti dalla sua riproduzione, trascrizione, esecuzione, rappresentazione, recitazione, comunicazione, distribuzione, traduzione, elaborazione, noleggio e prestito.

In secondo luogo, occorre considerare che "La rivoluzione digitale ha il potenziale per rendere fungibili, come merci nel ciberspazio, le esperienze culturali, proprio come il denaro ha reso fungibili lo scambio di beni nello spazio geografico"[121]. La digitalizzazione delle opere e la facilità di scambio dei prodotti culturali provocano, come già anticipato, l'inefficienza di qualsiasi sistema di appropriazione esclusiva dei beni immateriali, rendendo obsoleto il quadro normativo delineato dalla legge sul diritto d'autore.

Ecco dunque un altro parallelo tra copyright e privacy: il limite tecnologico. Potrebbe affermarsi, a tal proposito, che la tecnologia piega la legge, dovendosi intendere con tale espressione l'effetto modificativo che lo sviluppo cibernetico ha sulla normativa. Essa, infatti, non può prescindere da continui adattamenti in linea con quelli – rapidissimi – della materia regolata. I vincoli al comportamento umano, d'altronde, non sono solo limiti normativi. Come sostenuto da Lessig, infatti, interagiscono tra loro diversi limiti: la legge, le norme sociali, il mercato, l'architettura. Mentre i primi due aspetti sono già stati affrontati, vale soffermarsi sugli altri due. Il mercato, certo, può incidere su un fenomeno, qualunque esso sia, determinando un maggiore o minore consumo, scambio, utilizzo di un prodotto e alterando così quello che sarebbe spontaneamente accaduto, poiché fa dipendere le abitudini legate a quell'oggetto da elementi come prezzo, disponibilità, offerta, alternativa, distribuzione.

[121] Jeremy Rifkin, cit., p. 227; interesse privato comunque strumentale alla tutela di un interesse pubblico, ossia lo sviluppo della creatività e dell'innovazione (*cfr* infra).

Di tutt'altra fattura il limite imposto dall'architettura[122], che incide invece sulla struttura stessa dell'oggetto, imponendo ostacoli (o agevolazioni) di natura fisica, non aggirabili, alle quali è necessario sottostare non per scelta ma perché non è possibile fare altrimenti. "Il mondo fisico per come lo si trova", così lo chiama Lessig, obbliga ogni fenomeno, compreso quello tecnologico, a darsi dei limiti, dati dagli spazi fisici entro i quali può muoversi e oltre i quali non può andare (banalmente e generalizzando, lo spazio e il tempo, in tutte le loro accezioni cibernetiche). In conclusione, non esiste un solo vincolo ma più vincoli, tra i quali la legge assume senz'altro un ruolo dominante, pur senza che possa prescindere del tutto dagli altri fattori[123].

Per la *data protection* stiamo assistendo ad un fenomeno analogo, del quale ci occuperemo nel terzo ed ultimo capitolo.

---

[122] Daniel J. Solove, *No privacy*, cit.; Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 487; Daniel J. Solove, *The Digital Person - Technology And Privacy In The Information Age*, cit., p. 186.

[123] Lawrence Lessig, *Cultura libera*, Milano, Apogeo, 2005, http://www.liberliber.it/mediateca/libri/l/lessig/cultura_libera/html/testo.htm.

CAPITOLO III – IL GLOBAL PRIVACY STANDARD E IL *DATA SHARING*

Abbiamo delineato i due valori della privacy, la *privacy as intimacy* e la *privacy as identity*.

Collegato al primo valore troviamo un modello di tutela che abbiamo definito *privacy as dignity*: in caso di intromissione nella vita privata dell'individuo, la libertà negativa prevale salvo che non sia ravvisabile un interesse pubblico prevalente e siano rispettate le garanzie previste dalla legge o i parametri fissati dalla giurisprudenza. Tale modello trova applicazione sia rispetto alle questioni sulla sorveglianza sia rispetto a quelle sulla pubblicazione di fatti privati. Si tratta di un diritto individuale esercitabile *erga omnes*.

Collegato al secondo valore di identità contestuale abbiamo visto che il modello di tutela è quello che abbiamo definito *privacy as confidentiality*, dove la tutela immediata dell'identità dell'individuo (e soltanto mediata della sua intimità) passa attraverso l'imposizione di alcuni obblighi sul *data holder*: limitazione, trasparenza, base legale e sicurezza. Analizzando tale modello di tutela, abbiamo argomentato che esso dovrebbe fondarsi sul concetto di identità contestuale, vale a dire sulle norme sociali e giuridiche di appropriatezza e circolazione dei dati condivisi in un determinato contesto (*privacy as contextual identity*). Si tratta di un diritto dipendente dalla relazione tra *data subject* e *data holder.*

In un contesto digitale entrambi i valori sono messi in pericolo: l'intimità da quella che possiamo definire sorveglianza di massa e l'identità contestuale da quella che abbiamo definito l'iper-identità (digitale), entità che

sembra essere slegata sia da un certo contesto sia da una cornice temporale.

Grazie all'analisi di un altro ambito messo in crisi dalla rivoluzione digitale, ossia la disciplina della proprietà intellettuale, abbiamo constatato che: (i) gli strumenti di tutela coincidono spesso con i dispositivi tecnici volti ad impedire certe facoltà all'utente e la tutela giuridica diviene la tutela di questi dispositivi; (ii) oltre al limite normativo, occorre sempre considerare i limiti imposti dal mercato e dall'architettura.

Nella terza parte di questa tesi passeremo prima in rassegna i principi del Global Privacy Standard (*privacy as confidentiality*) e quindi proveremo ad elencare una tassonomia delle questioni legate alla privacy oggi.

1. Il Global Privacy Standard oggi

Il sistema di *data protection* a livello internazionale, ossia il Global Privacy Standard (GPS), è oggi costituito da quattro principi fondamentali, consacrati nella Dichiarazione di Madrid del 2009. Questi stessi principi sono i capisaldi della già citata convenzione di Strasburgo (1981), della prima Direttiva europea (1995), del Codice Privacy canadese (1996), dell'accordo di Safe Harbor tra Stati Uniti e Unione europea (2000), dell'accordo quadro sulla privacy dell'*Asia-Pacific Economic Cooperation* (2004) e sulle raccomandazioni in materia di *Binding Corporate Rules* del *Working Party* 29 (2008)[124]. Li analizziamo separatamente cercando di mettere in luce i

[124] Tim Wafa, *Global Internet Privacy Rights: A Pragmatic Approach*, University of San Francisco Intellectual Property Law Bulletin, 2009, p. 146 e ss.

vari corollari.

Il primo, o principio di limitazione (o *data minimization*): nella convenzione di Strasburgo (art. 5) ci si riferisce a questo principio anche con l'espressione di "*Data Quality*". In senso sincronico e diacronico il *data holder* deve trattare i dati (e solo quei dati) pertinenti ad una certa finalità. A tale principio si fa riferimento anche quando si parla di "proporzionalità" e "necessarietà". Il principio generale è quindi che la raccolta dei dati deve essere minimizzata in base al principio di necessità e proporzionalità che impone, a priori, (1) di raccogliere esclusivamente le informazioni (relative a un individuo) direttamente pertinenti e necessarie per raggiungere l'obiettivo specificato (in ossequio al già citato principio di finalità) e, a posteriori, (2) di conservare i dati per il tempo strettamente necessario a questo adempimento. Ne discende, per quello che possiamo definire principio di necessità a priori (descritto *sub* 1), che "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità" (art. 3 Codice Privacy italiano). Si tratta di una buona definizione del concetto di *privacy by design*: i sistemi informativi, i dispositivi e gli oggetti intelligenti che raccolgono dati devono essere progettati e realizzati sin dall'inizio in modo da limitare al massimo la raccolta d'informazioni, evitando raccolte di dati ulteriori e non pertinenti rispetto allo scopo perseguito. Ann Cavoukian, *Information & Privacy Commissioner* dell'Ontario cui si deve tale concetto, lo definisce efficacemente come la "*do nothing option*":

l'interessato non deve fare nulla perché il trattamento dei dati deve essere già impostato al livello minimo di raccolta dei dati in relazione a una certa specifica finalità. Sarà poi l'interessato che, se vorrà, potrà condividere un maggior numero di informazioni. Ne discende anche, per quello che possiamo definire principio di necessità a posteriori (descritto *sub* 2), che la proposta di una data di scadenza per le informazioni[125] (il metadato associato alle nostre informazioni personali, di cui abbiamo già parlato) è già conforme a diritto e corrisponde a una diversa regolamentazione della cosiddetta *data retention*. Al riguardo si è anche parlato di ecologia dell'informazione (o dell'info-sfera) e di strumenti di limitazione dell'inquinamento informativo.

Si tratta di metafore interessanti per descrivere ciò che in realtà sta avvenendo: ad esempio nei siti di social network assistiamo alla condivisione indiscriminata di informazioni per un lasso di tempo in relazione al quale non si hanno concrete garanzie. Sembra difficile che la *social privacy* (ossia la privacy dei social network) sia concepita in termini di *privacy by design*.

Ecco che, sincronicamente, la norma richiede che il trattamento dei dati, raccolti e gestiti in materia leale e legittima, debbano essere usati solo per finalità legittime ed entro un perimetro di rilevanza, adeguatezza e non eccessività (proporzionalità) delineato proprio dalla finalità del trattamento. La finalità del trattamento è

[125] Un principio analogo a quello di privacy by design è quello dell'ecologia dell'informazione: vedi Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, cit., p. 136 e ss. Da questo concetto deriva anche la possibilità che la limitazione dell'uso di questi datti abbia una dimensione sia sincronica sia diacronica, ossia una data di scadenza (p. 158).

condividere le informazioni con varie cerchie di persone (amici, conoscenti, pubblico). I *privacy settings* dovrebbero consentire di regolare il livello di diffusione delle informazioni. In senso diacronico, i dati devono essere aggiornati e utilizzati per il tempo necessario al raggiungimento della finalità. L'ambizione dei social network, tuttavia, è diventare il diario eterno dei propri utenti, dalla nascita alla morte (è il tema dell'eredità digitale).

In ogni caso, chi dovrebbe garantire i diritti del *data subject*? Il principio di finalità, a ben vedere, delinea esattamente anche la definizione di *data controller*. Il titolare del trattamento è (*ex* Convenzione di Strasburgo, art. 1) il soggetto che ha il potere di decidere giustappunto la finalità dei dati e quindi la categoria delle informazioni necessarie e le operazione da compiersi sugli stessi. Il *data controller* correlativamente è il soggetto su cui incombono i già noti obblighi di trasparenza e confidenzialità.

Inoltre, sempre a partire dal principio di *data minimization,* esistono insieme di dati che richiedono tutele rafforzate? La risposta è ovviamente positiva e riguarda il tema dei dati sensibili (o *sensitive data*), ossia di speciali categorie di dati (articolo 6 della Convenzione di Strasburgo), ossia quelli relativi alla razza, alle opinioni politiche, religiose e filosofiche, alla salute, alla vita sessuale e alle condanne penali, in grado di incidere in maniera determinante sulla nostra identità. Continuando nell'esempio dei social network, la finalità di questi siti è proprio rappresentare la nostra identità nella maniera più aderente possibile: quindi le nostre opinioni e le nostre preferenze.

In sintesi: il trattamento di dati personali è consentito entro il perimetro di quanto è necessario (principio di necessità o proporzionalità) in relazione a uno specifico

fine (principio di finalità); i principi di proporzionalità e di finalità servono a parametrare anche la qualità dei dati, posto che i dati devono essere pertinenti, completi, aggiornati e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.

Il secondo, o principio di trasparenza: l'art. 8 della Convenzione di Stasburgo comincia a delineare il principio di trasparenza assegnando all'interessato quattro diritti fondamentali: anzitutto (i) il diritto a sapere dell'esistenza di una banca di dati (preoccupazione che era stata la prima e più importante del legislatore svedese nel primo *data act* della storia), quindi (ii) il diritto ad accedervi, (iii) il diritto a ottenere la rettificazione dei dati e (iv) il diritto di ottenerne la cancellazione in caso di violazione della normativa sulla *data protection*. Possiamo quindi distinguere due aspetti del principio di trasparenza: in primo luogo principio di trasparenza preventiva, in forza del quale il trattamento di dati personali è consentito solo se preceduto da adeguata informativa che chiarisca le finalità del trattamento (saldando principio di limitazione e principio di trasparenza); in secondo luogo principio di trasparenza successiva: il trattamento dei dati è consentito solo se, una volta effettuata la raccolta delle informazioni, si dà la possibilità all'interessato (*data subject*) di accedere ai propri dati e controllarne la qualità, come sopra definita, e solo se il titolare del trattamento (*data holder*) assicura appositi meccanismi per garantire tale accesso e il riscontro alle richieste dell'interessato. La centralità di questo principio ed il suo collegamento con il principio di limitazione chiarisce perché la *data protection* è, in definitiva, uno strumento di "trasparenza" posto a tutela della *privacy as (contextual) identity* mentre il diritto alla riservatezza posto a tutela della *privacy as intimacy* è uno strumento di opacità.

Il terzo, o principio di base legale: il trattamento deve poggiare su una base legale. In questo caso riemerge la distinzione tra contesto pubblico e privato: infatti in relazione a trattamenti di soggetti pubblici (statuali) la base legale sarà la legge; in relazione a trattamenti di soggetti privati la principale base legale sarà il consenso dell'interessato. Il principio del consenso, tuttavia, viene temperato da una serie di importanti eccezioni: richiesta dell'interessato (in fase precontrattuale e/o contrattuale); legittimo interesse del *data holder* (ad esempio in materia di esercizio di un diritto in giudizio).

Anche il principio di base legale deve essere visto in stretta correlazione con il principio di *data minimization* e con la *transparency rule* che abbiamo appena descritto. Il consenso, ad esempio, dovrebbe collegarsi a una specifica finalità, resa esplicita da un'informativa chiara e facilmente accessibile per l'interessato.

Possiamo aggiungere che il consenso deve essere libero e ciò pone diversi problemi in relazione all'autorizzazione al trattamento dei dati, ad esempio, in ambito aziendale o al consenso prestato dai minori. Molto spesso, in questi casi, la base legale del trattamento delle informazioni personali potrà essere solo una legge.

Proprio con riferimento al consenso possiamo considerare i limiti imposti dall'architettura e dal mercato. Su Internet il consenso (spesso un semplice e poco consapevole *point and click*) è la migliore base legale? Il consenso deve essere esplicito (cosiddetto "*opt-in*") o può essere anche implicito ("*clear affirmative action*")? Può bastare la semplice richiesta di un servizio dell'interessato? Il nostro comportamento digitale è oramai legato ad una serie di servizi (e-mail, calendari *web based*, piattaforme di contenuti) che richiede la cessione di informazioni, alcune personali. L'informazione-struttura è

concepita proprio per archiviarle, per organizzarle e per renderle disponibili nella maniera più efficiente possibile. L'architettura di Internet è proprio votata al *data sharing*.

Aggiungiamo a questa constatazione anche il vincolo economico. Il nostro comportamento digitale è ulteriormente condizionato dalla falsa convinzione che questi servizi siano "gratuiti". Uno dei paradigmi da studiare è quindi il modello di business sottostante la possibilità di accedere a questi servizi senza pagare, che non vuol dire necessariamente "gratuitamente"[126].

Come è noto, infatti, il principale modello di business presente su Internet riguarda lo scambio tra un servizio (o un contenuto) al quale l'utente accede e la cessione di dati personali che verranno utilizzati per finalità commerciali. La domanda è: dovremmo consentire a questo modello o dovremmo esserne solo pienamente consapevoli, potendo quindi scegliere più radicalmente di non accedere al servizio. Il consenso, in quest'ottica, dovrebbe essere necessario solo in particolari casi. Il punto essenziale, infatti, è la velocità della transazione (cessione di dati personali/erogazione del servizio) nel contesto di Internet. Si dovrebbe individuare un sistema facile e intuitivo per comprendere il contesto nel quale ci si trova (*transparency rule*) e, solo in casi eccezionali, esprimere il proprio consenso. Si dovrebbe rendere estremamente chiaro il perimetro del trattamento consentito dall'utente al *data holder* in relazione al principio di finalità: la finalità funzionale (servizi di base o servizi aggiuntivi per l'utente – ad esempio, la geolocalizzazione che consente di accedere a servizi di segnalazione di esercizi commerciali); la finalità commerciale (*advertising*); la finalità di

[126] Eugene Volokh, cit., p. 1118.

profilazione (analisi e previsione di comportamenti dell'utente). La prima finalità dovrebbe avere una base legale diversa dal consenso; le ultime due finalità tradizionalmente richiedono il consenso. Ulteriore problema riguarda il consenso al trattamento di particolari categorie di dati che, in Europa, dovrebbe essere scritto e autorizzato dall'Autorità amministrativa di garanzie (il Garante per la protezione dei dati personali).

Il quarto e ultimo principio è quello di sicurezza dei dati: l'art. 7 della Convenzione di Strasburgo pone il principio di *data security*. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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. In particolare, si tratta per il *data holder* di adoperarsi per garantire la sicurezza delle sue banche dati: sono i temi dell'adozione di procedure di gestione delle credenziali di autenticazione (sistema di autenticazione anche informatica); dell'utilizzazione di un sistema di autorizzazione; dell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (profilo di autorizzazione); della protezione fisica e tecnica degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (*firewall* e antivirus); dell'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi (*back up*

e *disaster recovery*); dell'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Quanto al sistema di autenticazione, il trattamento di dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato (*user id*) associato a una parola chiave riservata (*password*). *User id* e *password* possono essere sostituite da un dispositivo di autenticazione in possesso e a uso esclusivo dell'incaricato, eventualmente ed ulteriormente associato a un codice identificativo o a una parola chiave (si pensi ad un *token* o un dispositivo cellulare che riceve via sms la password), oppure dall'individuazione di una sua caratteristica biometrica, eventualmente sempre associata a un codice identificativo o a una parola chiave. A ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione che non devono essere assegnate o associate ad altri.

L'incaricato riceve una serie di indicazioni impartite per iscritto che costituiscono il suo profilo di autorizzazione; unitamente al profilo gli è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in suo possesso e uso esclusivo, nonché relative alla custodia e all'accessibilità dello strumento elettronico durante una sessione di trattamento. In caso di impedimento o assenza prolungata, procede il custode delle copie delle credenziali, anche in questo caso

in modo del tutto trasparente sia preventivamente (l'incaricato viene informato per iscritto nel suo profilo di autorizzazione) sia successivamente (al momento dell'intervento, l'incaricato riceve una comunicazione). Le credenziali devono essere disattivate in caso di perdita della qualità che consentono all'incaricato l'accesso ai dati personali.

Nel complesso, i profili di autorizzazione costituiscono il sistema di autorizzazione. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati prima dell'inizio del trattamento e periodicamente verificati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento (altra manifestazione del principio di necessarietà o proporzionalità)[127].

Il Global Privacy Standard pone dunque al centro la figura del *data holder*: verso l'esterno e nei confronti del *data subject*, egli deve rispettare tre principi fondamentali e strettamente collegati tra loro - limitazione, trasparenza e base legale -; all'interno della propria organizzazione, invece, egli deve adottare le misure di sicurezza adeguate, basate sul sistema di autenticazione e sul sistema di autorizzazione, volte ad impedire trattamenti illeciti di dati. Possiamo descrivere questo modello di tutela in altro modo: per garantire l'identità del *data subject*, il *data holder* deve chiarire il contesto del trattamento (parliamo quindi di identità contestuale) e di rispettare un obbligo di confidenzialità su quei dati.

---

[127] Accanto a questi quattro principi fondamentali, i trattati internazionali pongono sempre il problema della giustiziabilità di questi diritti (vedi art. 8 lett. d della Convenzione di Strasburgo). David H. Flaherty, cit., p. 10.

2. Il Global Privacy Standard domani: la tassonomia della privacy al tempo del *data sharing*

Piuttosto che partire da una definizione unitaria di privacy, bisogna prendere atto delle varie accezioni del termine: *privacy as intimacy*, privacy verticale, privacy orizzontale, *privacy as identity*, *spatial privacy*, *privacy as dignity*, *privacy as property*, *privacy as confidentiality*, *privacy as contextual identity* e *privacy as copyright*, solo per citare quelle che abbiamo utilizzato in questa tesi.

Un primo tentativo di classificare i vari modelli di tutela della privacy era stato operato dal già citato William Prosser che, nel 1960, aveva raggruppato tutte le azioni che riguardavano la *tort privacy* (con un *focus*, dunque, sull'approccio civilistico). Nel farlo, egli aveva volutamente trascurato la dimensione della *constitutional privacy*, già ben presente nella tradizione statunitense; non aveva potuto analizzare, inoltre, la *data base privacy* e in generale il trattamento automatizzato di informazioni personali che di lì a un decennio avrebbe posto nuove questioni, così come non aveva potuto prevedere le incredibili sfide poste dall'era di Internet[128]. Tuttavia proprio a partire dal lavoro di Prosser possiamo tracciare una linea di demarcazione tra i modelli di tutela delle prime due tipologie di attività che abbiamo considerato (*hard privacy*) e delle ultime due (*soft privacy*). A partire dagli anni '70 l'archiviazione e la circolazione di informazioni personali hanno rappresentato la principale minaccia a quella che, sui media e nell'opinione pubblica,

[128] Neil M. Richards e Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, cit., p. 1907.

viene definita privacy; negli anni ’90, poi, una serie di nuovi problemi è sorta a causa delle nuove tecnologie informatiche sempre con riferimento alla memorizzazione e alla circolazione dei dati personali.

L’opera di Prosser chiarì che il diritto alla privacy era invocato a proposito di controversie molto diverse tra loro e non pareva essere riducibile a un’unità. Ciò è tanto più vero ove si consideri che, negli ultimi cinquat’anni, abbiamo visto ulteriormente sfaccetarsi le pretese che alla privacy fanno riferimento e ulteriormente sovrapporsi norme di rango costituzionale, fattispecie penali, norme civilistiche.

Daniel Solove, nel 2006[129], ha raggruppato in quattro categorie le attività che mettono a rischio la privacy: il primo gruppo, chiamato “*information collection*” ricomprende l’osservazione, l’ascolto o la registrazione delle attività degli individui e le varie forme di raccolta di informazioni; un secondo gruppo di attività, l’“*information processing*”, riguarda invece il trattamento dei dati successivo alla raccolta, compresa la loro aggregazione e combinazione per finalità di profilazione; un terzo gruppo di attività riguarda la diffusione di informazioni private o comunque riservate (in ogni caso veritiere, giacché ciò distingue, come già scritto, la tutela della privacy dalla tutela dell’onore e della reputazione); infine un quarto gruppo ricomprende tutte le intrusioni di terzi nella sfera privata degli individui. Possiamo quindi confrontare la classificazione fatta da Solove con i modelli di tutela qui descritti: (i) l’*information collection*, ossia l’archiviazione dei dati attraverso attività di controllo oppure di raccolta di dati, e (ii) l’*information processing* mettono a rischio la

[129] Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 484.

privacy positiva – *privacy as identity* – e accedono a un modello di tutela che abbiamo definito *privacy as confidentiality* riletta alla luce dell'identità contestuale; (iii) la divulgazione di informazioni private e (iv) le intrusioni ingiustificate in spazi o fatti privati impattano sulla privacy negativa – *privacy as intimacy* – e comportano un modello di tutela che abbiamo definito *privacy as dignity*.

Nei primi due casi abbiamo focalizzato l'attenzione su un ambiente relazionale che traccia lo statuto di limitata accessibilità/disponibilità delle informazioni. Negli altri due casi è piuttosto la delimitazione tra perimetro privato e perimetro pubblico a venire in rilievo: la libertà privata deve essere salvaguardata (e quindi i dati devono essere considerati privati) salvo che non vi sia un interesse pubblico a comprimere detta libertà sempre nel rispetto di garanzie legali per quanto riguarda la privacy verticale, ossia nel rapporto tra Stato e individuo, e in ossequio ad un generale principio di necessarietà per quanto riguarda la privacy orizzontale, ossia nel rapporto tra collettività e individuo. Per converso, analizzando la medesima situazione giuridica da un altro angolo visuale, le informazioni accessibili alla collettività o che riguardano l'azione dello Stato devono essere caratterizzate da uno statuto di generale accessibilità/disponibilità. Si tratta di un tema di grande importanza che purtroppo esula dall'oggetto del presente lavoro.

Peraltro, oggi tutti i concetti che abbiamo utilizzato devono essere riconsiderati in un nuovo contesto digitale, non più dominato dalle banche di dati, ma dai nuovi sistemi convergenti di comunicazione: tracce volontarie e involontarie che vengono lasciate in una nuova sfera sociale, non (solo) privata e non (solo) pubblica. La quantità di informazioni personali cresce

esponenzialmente (ipertrofia informativa) e aumenta la possibilità di accedervi (iperaccessibilità informativa)[130].

La tassonomia della privacy cui abbiamo fatto riferimento come inquadra il problema della digital privacy? Sappiamo che dal classico angolo visuale della *data protection* la questione è principalmente di controllo sui propri dati personali e, quindi, sulla propria identità. Riteniamo tuttavia che sia più utile parlare del rapporto tra *data holder* e *data subject* nei termini di una nuova confidenzialità posta a protezione dell'identità contestuale.

Possiamo quindi proporre una diversa classificazione che non tragga origine né dai possibili rimedi a violazioni della privacy (come fatto da Prosser) né dalle possibili azioni che la mettono in pericolo (come fatto da Solove), quanto piuttosto dai rapporti tra soggetti portatori di interessi contrapposti.

Abbiamo già considerato che il *right to privacy* in senso tradizionale è un diritto individuale esercitabile *erga omnes*. Abbiamo quindi analizzato la *data protection* a partire dal rapporto tra *data subject* e *data holder* e abbiamo declinato gli obblighi di quest'ultimo. Accanto a tali soggetti, per impostare la nostra tassonomia, dobbiamo introdurre una terza categoria di portatore di interessi alla raccolta e all'uso delle informazioni. Se, infatti, il *data subject* è il soggetto portatore dell'interesse a mantenere il controllo sulle proprie informazioni e se il *data holder* è il soggetto che ha un interesse, qualificato secondo noi da una cornice di confidenzialità[131], alla raccolta e all'uso

---

[130] John Palfrey e Urs Gasser, *Nati con la Rete*, Milano, 2009, p. 64.

[131] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 179; Helen Nissenbaum, *Privacy as contextual integrity*, cit., p. 124 e ss.

delle informazioni, quando tale cornice manca e rileviamo un conflitto in materia di privacy vi sarà sempre un portatore di interessi confliggenti con quello del *data subject*. Utilizzando la terminologia economica possiamo definirlo *stakeholder*. La differenza tra *data holder* e *stakeholder* è, dunque, la cornice di confidenzialità.

Prima di passare a considerare i vari rapporti, occorre riprendere l'analisi dei valori sottostanti. L'ipotesi che abbiamo formulato è che vi siano almeno due valori fondamentali che vengono evocati dal concetto di privacy ed è questo, riteniamo, il motivo per cui il Global Privacy Standard è ben lungi dal riferirsi alla disciplina di tutte le minacce alla privacy che vengono quotidianamente paventate. Si avranno, quindi, da un lato attività potenzialmente lesive degli spazi privati (e della libertà) dell'individuo e, dall'altro, attività potenzialmente lesive dell'identità personale di ciascuno (la privacy in senso positivo). Il Global Privacy Standard, nato dalla *data base privacy*, si occupa di regolare queste ultime attività o, meglio, pone alcuni obblighi sui detentori delle banche di dati (il *data holder*). E ora che Internet è una gigantesca banca dati si chiede con forza la protezione della *digital privacy*, ossia di quei dati che i *data holder* della Rete memorizzano e utilizzano per le loro finalità. Bisogna preoccuparsi, come detto, della propria iper-identità digitale, ossia delle informazioni trattate da un sistema informatico che sono memorizzate sui server sparsi nel mondo.

I concetti di privato e pubblico in questo contesto rischiano di essere riduttivi e fuorvianti ed emerge piuttosto la relazione tra *data subject* e *data holder*, con quest'ultimo che dovrà garantire l'identità parziale (noi l'abbiamo definita contestuale) del primo.

In questo contesto, affermare un diritto individuale al controllo dei propri dati personali appare del tutto vano, oltre che di difficile (se non impossibile, come qui si ritiene) realizzazione. Un primo livello di protezione si manifesta nel rapporto tra *data subject* e *data holder*. L'interesse del *data subject* a plasmare la propria identità deve essere tutelato dal *data holder* ed in caso di violazione il relativo diritto deve essere esercitato contro il *data holder* in base alla confidenzialità del trattamento di dati personali. Neppure ha senso dire che si tratti di un problema analogo a quello del *copyright*, ossia una sorta di autorizzazione o licenza all'uso dei dati personali che il *data subject* rilascia al *data holder*. L'identità non è un bene di cui possiamo disporre in via esclusiva, come un'automobile, l'identità è un bene fatto per essere condiviso (quindi inclusivo) che vogliamo sia rispettato nella sfera pubblica. Non si vede, infatti, per quale ragione dovrebbe essere presente un obbligo di trasparenza successiva, cioè un diritto di accesso a quei dati o un diritto di richiesta di correzione e di opposizione al loro utilizzo. Se fossimo in presenza di un diritto analogo a quello di *copyright*, avremmo diritti ben più penetranti (anche se sostanzialmente inefficaci in un contesto digitale). Il paradigma proprietario pare, pertanto, non adeguato a spiegare e risolvere i conflitti in materia di *data protection*.

Venendo alla tassonomia che proponiamo, l'idea fondamentale è che la privacy ponga sempre due ordini di temi: un tema di misura della libertà individuale e un tema di controllo della propria identità. Libertà negativa e libertà positiva. Necessità di evitare intrusioni nella sfera privata dell'individuo ed esigenza di controllare i propri dati personali nella sfera pubblica. Occorre allora ricostruire e avere in mente almeno tre rapporti giuridici:

quello tra *data holder* e *data subject* che ci pare caratterizzi il dibattito sull'identità e quindi sulla libertà positiva; quello tra *data subject* e *stakeholder* (ossia soggetto controinteressato alla raccolta e all'utilizzo dei dati) e quello tra *stakeholder* e *data holder*, nel momento in cui lo *stakeholder* voglia raccogliere i dati del *data subject* presso il soggetto che li detiene in una banca dati che ci pare ponga una questione di intimità e di libertà negativa. Avendo in mente questi tre rapporti giuridici è possibile esaurire le questioni in materia di privacy, intesa in senso ampio, riconoscendo il relativo modello di tutela.

Nel primo caso, troverà applicazione la disciplina sulla *data protection* che impone un obbligo di trasparenza volto a delineare il contesto in cui l'archiviazione e l'uso dei dati avvengono e un dovere di confidenzialità, ossia di limitazione nell'uso di questi dati in riferimento ad una certa finalità. Qualsiasi decontestualizzazione dovrà poggiare su una base legale che, nei rapporti tra privati, sarà il consenso dell'interessato. Quella appena enunciata è già oggi la regola concretamente applicabile, anche se attraverso un percorso molto più tortuoso. La regola generale vuole che il trattamento tra privati debba essere acconsentito salva l'applicabilità delle tante eccezioni previste, tra cui quella in forza della quale non è necessario il consenso quanto il trattamento dei dati è necessario per eseguire obblighi derivanti da un contratto del quale è parte il *data subject* o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato. È difficile che in casi di decontestualizzazione delle informazioni, ossia di raccolta e di utilizzo dei dati per finalità diverse da quelle rese trasparenti nell'informativa e non acconsentite, si debba o si possa parlare di lesione della libertà negativa del *data subject*. Nemmeno avrà senso fare riferimento alla

dicotomia pubblico/privato per farsi guidare nella soluzione dei vari casi.

Nella seconda ipotesi, abbiamo detto che il rapporto sarà tra *data subject* e *stakeholder* senza che vi sia una cornice di confidenzialità. Un buon esempio può essere fatto in tema di giornalismo: un giornalista (*stakeholder*) vuole diffondere notizie private o informazioni personali su un *data subject* che invece è contrario. Si tratterà allora di un tema di libertà ed interesse generale della notizia, ossia della possibilità garantita al *data subject* di sottrarsi dalla sfera pubblica in relazione a determinati contesti privati.

Vi è ancora una terza ipotesi, sempre più rilevante per la proliferazione delle banche dati. È il caso in cui lo *stakeholder* voglia raccogliere le informazioni non direttamente presso il *data subject* ma presso un *data holder*. Ciò può verificarsi, ad esempio, quando l'Autorità Giudiziaria richiede delle informazioni su un soggetto al gestore telefonico. In questo terzo e ultimo caso, entrerà ancora in gioco il tema della libertà e quindi delle garanzie a tutela del *data subject*; è il tema della *data retention*[132]. Le misure in tema di conservazione di dati di traffico telefonico e telematico per finalità di accertamento e repressione dei reati mostrano chiaramente la rilevanza di due rapporti: in primo luogo quello tra *data subject* e *data holder*, rapporto cui si applica la *data protection* e che rappresenta la prima ipotesi della nostra tassonomia; in secondo luogo quello tra *data holder* e *stakeholder* pubblico, ossia nel nostro esempio Autorità Giudiziaria,

[132] Neil M. Richards, *Intellectual privacy*, cit., p. 437 e ss. Per l'Autore questa terza ipotesi è definibile quale *intellectual privacy*. Daniel J. Solove e Chris Jay Hoofnagel, *A Model Regime Of Privacy Protection*, cit., p. 377 e ss.

caratterizzato da garanzie peculiari che nulla hanno a che vedere (e anzi sono in aperto contrasto) con i principi di limitazione, trasparenza e *data security*.

Tornando alla classificazione dei problemi legati alla *digital privacy*, pertanto, un primo insieme di conflitti deve essere risolto attraverso la corretta applicazione, da parte dei *data holder*, dei principi di limitazione, trasparenza, base legale e *data security* che si fondano, come abbiamo visto, sulla confidenzialità delle informazioni personali e sul rispetto dovuto all'identità contestuale dell'individuo. Sia le questioni di *information collection* sia quelle di *information processing* si collocano entro questo perimetro. Il contesto digitale nel quale ci muoviamo richiede tuttavia un aggiornamento dei principi di limitazione e di base legale. Nel primo caso, in modo analogo a quanto accaduto per il diritto d'autore, ciò avverrà attraverso soluzioni tecniche prima ancora che giuridiche: da un lato, l'approccio *privacy by design*[133], ossia l'incorporazione del principio di minimizzazione fin dalla progettazione dei dispositivi che debbono raccogliere o processare le informazioni e, dall'altro, le *privacy*

[133] Ovviamente l'approccio *privacy by design* non è solo questo, bensì trova articolazione in sette principi: prevenire i problemi legati alla privacy piuttosto che agire reattivamente; impostare di default la minimizzazione dei dati raccolti dando all'utente la possibilità di modificare tale impostazione (e non viceversa); come anticipato, incorporare il principio di minimizzazione nella stessa architettura IT e nelle varie pratiche commerciali; evitare i giochi a somma zero, ossia le contrapposizioni, ad esempio, privacy *vs* sicurezza, dimostrando che è possibile avere entrambe; garantire il rispetto di questi principi in tutte le fasi del trattamento e non solo nel momento iniziale della raccolta; garantire, altresì, la massima trasparenza; mettere al centro l'utente.

enhancing technologies[134] vale a dire mezzi tecnici quali la crittografia, le forme di anonimizzazione e di rimozione, gli strumenti di gestione della nostra identità, le procedure di segnalazione.

In relazione alla base legale, invece, in un contesto completamente interattivo come è il contesto digitale, dovrebbe perdere di centralità l'istituto del consenso, per privilegiare sia il legittimo interesse del *data holder* sia la richiesta, esplicita o implicita, dell'utente di fruire di un certo servizio. È chiaro che nel contesto digitale non è possibile richiedere per ogni interazione tra utente e macchina un consenso, giacché la funzionalità è estremamente importante e richiede un netto ripensamento del modello legale pensato negli anni settanta del secolo scorso per un'attività di raccolta e processazione delle informazioni nelle banche dati della pubblica amministrazione o delle grandi imprese. Proprio da questo punto di vista il rispetto dell'identità contestuale dovrà essere considerato il primo parametro di legittimità del trattamento, trattamento che quindi potrà trovare fondamento non solo nella legge o nel consenso ma anche nel legittimo interesse di un soggetto privato che offre un servizio su Internet o nel comportamento concludente

---

[134] Daniel Solove, *No privacy*, cit., p. 200 e ss. Communication from the Commission to the European Parliament and the Council on Promoting *Data Protection* by Privacy Enhancing Technologies (PETs); si veda anche http://ec.europa.eu/idabc/servlets/Doc?id=28587. Per un approccio pratico alle tecnologie di autenticazione PET si veda R. Leenes *2007 PRIME White Paper on Privacy-enhancing Identity Management*, 2007; https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V2.pdf. Vedi anche Marit Hansen, cit., p. 203.

dell'utilizzatore della Rete. Trasparenza e *data security*, invece, resteranno elementi imprescindibili della *digital privacy*, proprio perché sarà in evidenza un perimetro relazionale basato sulla fiducia e sul rispetto dell'identità contestuale dell'individuo.

Ovviamente non saranno soltanto questi i problemi della *digital privacy*. La storia di questo diritto, come abbiamo visto, è la storia della dimensione pubblica che invade la dimensione privata e della dimensione privata che invade la dimensione pubblica. Pertanto, un secondo insieme di conflitti dovrebbe essere risolto a partire dal modello della *privacy as dignity*. Quando la protezione dei dati non sarà garantita da una cornice di confidenzialità, dunque, emergerà lo schema che prevede la regolare prevalenza della libertà privata al riparo da interferenze esterne e di non vedere pubblicati fatti privati, salvo un interesse pubblico chiaramente identificato e, come più volte richiamato, nel rispetto delle garanzie previste per quanto riguarda la privacy verticale (rapporto Stato individuo) oppure con riferimento al parametro della necessarietà delle informazioni private (rapporto collettività-individuo) per il raggiungimento dell'interesse pubblico. Si tratta dei fenomeni della sorveglianza e del giornalismo di massa. Quel che è problematico, infatti, è la facilità e la lesività delle violazioni della privacy orizzontale al tempo di Internet: la diffusione di strumenti di registrazione e captazione, la moltiplicazione dei blog, dei social network e degli strumenti di condivisione, tutto ciò ha un tale impatto quantitativo su questo genere di

violazioni che si pone il problema di una ridefinizione qualitativa di concetti quali quelli di intimità ed identità[135].

Riprendiamo la tassonomia proposta e descriviamola in senso storico: in materia di privacy, il primo tema è la contrapposizione tra un *data subject* (soggetto cui si riferiscono i dati e portatore di un interesse alla sottrazione dei dati dalla dimensione pubblica) e uno *stakeholder* (portatore di un interesse contrapposto o controinteressato). Nella *tort privacy* lo *stakeholder* poteva essere individuato, ad esempio, nel giornalista; nella *constitutional privacy* con il potere pubblico statale. Successivamente, a partire dagli anni sessanta del secolo scorso, lo schema si arricchisce del *data holder*, ovvero del soggetto che detiene i dati del *data subject*, sia perché quest'ultimo glieli ha comunicati sia perché il primo li ha lecitamente raccolti. Si pensi al caso del fornitore di servizi telefonici che raccoglie dati relativi alle comunicazioni di un soggetto. Ricapitolando: storicamente il primo gruppo di questioni attiene al rapporto tra interessato e controinteressato (*data subject* e *stakeholder*), il secondo tra *data subject* e *data holder*. Accanto a questi due insiemi di potenziali controversie in materia di privacy ve ne può essere un terzo: ossia quando lo *stakeholder* pretende di accedere ai dati del *data subject* detenuti dal *data holder* ponendo quindi un tema di libertà negativa dell'interessato rispetto al rapporto giuridico tra *data holder* e *stakeholder*. Anche qui la confidenzialità offre un interessante spunto problematico: una maggior tutela della confidenzialità, e quindi del rapporto tra *data subject* e

---

135 Morozov, http://www.corriere.it/cultura/12_febbraio_16/morozov-una-polizza-per-reputazione_e1bbac0a-5870-11e1-9269-1668ca0418d4.shtml.

data holder, implica in questo caso una maggior tutela della libertà negativa del *data subject* nei confronti dello *stakeholder* mediata dal *data holder*. Ossia: il *data holder* potrà (e dovrà) rifiutare allo *stakeholder* le informazioni sul *data subject*. Si tratta di uno snodo fondamentale oggi: il potere pubblico mira a controllare i gradi operatori privati che raccolgono informazioni sui loro utenti.

I problemi di diffusione di questi dati e di intrusione nell'altrui vita privata potrebbero sorgere al momento delle intercettazioni di queste comunicazioni. In questo caso, come detto, il controinteressato (o *stakeholder*) è lo Stato. Caso diverso è quello in cui il controinteressato richiede al *data holder*, ad esempio, i dati relativi al traffico telefonico, ossia dati che riguardano solo alcune caratteristiche esteriori delle conversazioni telefoniche senza permettere di prendere cognizione dei contenuti. Tuttavia, tali dati permettono di desumere altre informazioni: il destinatario della comunicazione, il momento e la durata della conversazione, persino la localizzazione dell'interessato in caso di uso di dispositivi mobili, per non parlare dei dati di traffico telematico che consentono di raccogliere informazioni ancora maggiori. Vi è, quindi, un impatto sulla libertà di comunicazione; per tale ragione, anche in questo caso dovrebbe applicarsi il modello di tutela che abbiamo definito *privacy as dignity*. I dati devono essere conservati dal *data holder* nell'ambito del proprio rapporto di confidenzialità e possono essere condivisi con il potere pubblico statuale solo in presenza di un chiaro interesse pubblico previsto da una legge e nel rispetto di specifiche garanzie. La disciplina europea della *data retention*, sotto quest'aspetto, limita l'accessibilità solo ad alcuni dati specificamente individuati, per un certo periodo di tempo e in forza di determinati provvedimenti dell'Autorità Giudiziaria.

3. Oltre il pubblico ed il privato: la confidenzialità come modello di tutela e l'identità contestuale come valore

Il Global Privacy Standard si basa su quattro principi che sono quattro obblighi imposti al *data holder*: limitazione, trasparenza, base legale e sicurezza. Ciò che vogliamo suggerire è una rilettura di questi principi alla luce del principio di identità contestuale e quindi nell'ottica di evitare la decontestualizzazione (sincronica e diacronica) delle informazioni che riguardano l'individuo. La stessa confidenzialità si riferisce, nella tradizione giuridica inglese, solo a determinati rapporti (tra medico e paziente; tra avvocato e cliente) e a certe informazioni[136]; mentre, come spiegato, quello di cui si tratta in questa sede è il dovere di confidenzialità generalizzato nei rapporti tra *data subject* e *data holder* al momento della memorizzazione e della circolazione dei dati personali con un aggiuntivo dovere di trasparenza volto a chiarire il contesto entro cui avviene lo scambio di informazioni. Riteniamo che questo sia il cuore della *data protection* e da qui si debba partire per affrontare la sfida della *digital privacy*.

Facendo un passo indietro nell'evoluzione dei diritti così come sviluppatisi oltreoceano, è interessante notare come già fossero insiti nelle due facce della "medaglia privacy" i problemi principali che ancora oggi rivestono grande attualità, poiché non completamente risolti. La *tort*

[136] Neil M. Richards e Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, cit., p. 134; Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 525; Neil M. Richards e Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, cit., p. 1909.

privacy, in particolare, aveva sottolineato la minaccia della diffusione di informazioni private sui mass media e il danno che ciò avrebbe potuto provocare; d'altro canto, la *constitutional privacy* aveva fissato le garanzie a tutela dell'individuo nei casi di invasioni ingiustificate degli spazi tradizionalmente considerati privati: la vita familiare, la casa, le comunicazioni a distanza; tema, quest'ultimo, che assume una nuova veste nel momento in cui non è più solo lo Stato a possedere strumenti di sorveglianza, tanto da far parlare, oggi, di sorveglianza diffusa.

In entrambi i casi ci si concentra sul rapporto e sulle frizioni tra l'individuo e la collettività cui l'individuo appartiene. Il principio alla base della relazione-opposizione tra il privato e il pubblico è che la quota di libertà individuale possa essere sacrificata solo in presenza di un interesse pubblico maggiore e, quindi, prevalente. Una prima protezione di questa libertà è stata di tipo fisico, grazie al muro salvaguarda ciascuno dagli sguardi altrui (*spatial privacy*): il diritto di proprietà diventava una prima barriera giuridica di fronte all'intrusione non autorizzata. La seconda barriera era prettamente giuridica, in base ad obblighi di riservatezza non più legati al contesto privato ma pattuiti concordemente tra due (o più) soggetti (*privacy as confidentiality*). L'inadeguatezza di queste due forme di tutela aveva portato alla terza barriera, anch'essa normativa, sancita dall'affermazione del diritto alla privacy come prerogativa dell'individuo esercitabile *erga omnes* sui propri sentimenti privati e teorizzata per la prima volta da Warren e Brandeis (*privacy as property*). Rispetto a questi presidi relativi alla privacy che abbiamo definito orizzontale, le Costituzioni dei vari Paesi ponevano precisi limiti al potere statuale, ossia dei limiti allo scrutinio pubblico statuale nella vita privata delle persone (privacy verticale). Tali considerazioni facevano

emergere una diversa concezione della privacy lontana dal modello proprietario e più attenta al valore dell'intimità: l'abbiamo definita *privacy as dignity*. Si ottiene, così, un quadro in cui l'architettura fisica, sociale e normativa delimita gli spazi e gli ambiti divenuti inaccessibili e indisponibili per altri diversi dal titolare del diritto. Si tratta di quella che la giurisprudenza statunitense chiama "ragionevole aspettativa di privacy"[137], cruciale nel diritto costituzionale degli Stati Uniti nel definire la portata della protezione della libertà privata. Infine, la preoccupazione per i trattamenti automatici di dati personali ha fatto emergere una nuova forma di confidenzialità (*privacy as new confidentiality*) negli obblighi che gravano sul *data holder* al momento della raccolta e dell'utilizzo delle informazioni personali che costituiscono l'identità dell'individuo (*privacy as identity*).

Questa carrellata storica rende evidente che non è utile – né giuridicamente corretto – riferirsi in termini generali a un diritto alla privacy.

Ne è un esempio eclatante il Global Privacy Standard che riguarda solo la *data protection* e la *soft privacy*. Abbiamo chiarito come la legge tuteli la privacy negativa, garantendole delle protezioni specifiche volte essenzialmente a limitare il potere statuale di interferire nei comportamenti e nelle scelte riguardanti la vita familiare delle persone (la casa che abitano, le comunicazioni a distanza, ecc.); rispetto a questi contesti, la sorveglianza si è diffusa e massificata, erodendo la quota di libertà privata riconosciuta a ciascuno. Un punto fisso però resta: il

[137] Lior Strahilevitz, *A Social Networks Theory of Privacy*, in *University of Chicago Law School*, 2004, p. 5 e ss; Vittorio Fanchiotti, *U.S. v. Jones: una soluzione tradizionalista per il futuro della privacy?*, in *Diritto penale e processo*, 2012, p. 381 e ss.

modello normativo è sempre quello che promana direttamente dai principi della Carta Costituzionale e dai Trattati internazionali e che si traduce nelle normative statuali – non globali - in ipotesi di reato e quindi di responsabilità penale. Un altro esempio di rapporto fortemente critico è quello tra diritto dell'informazione e libertà privata; anche in questo caso molto dipende dalla società in cui si svolge tale dibattito. Nondimeno il principio resta quello per cui l'interesse privato può venir sacrificato solo in presenza di un interesse pubblico prevalente, in base a parametri di essenzialità del fatto privato da divulgare rispetto all'interesse pubblico da far valere[138]. Anche in questo caso, la forte caratterizzazione politica dell'*hard privacy* (quale quota di libertà privata l'ordinamento riserva agli individui) rende difficilmente attuabile un Global Privacy Standard.

Nella nostra tassonomia, questi temi rappresentano un problema di libertà negativa in un rapporto giuridico contrassegnato dalla presenza tra uno *stakeholder*, da un lato, e un *data subject* o un *data holder* dall'altro. Nel momento in cui un governo cerca di accedere ai dati dei suoi cittadini, spiandoli o cercando di spiarli tramite le banche dati di operatori privati, si pone un problema di libertà e quindi di garanzie costituzionali. La *privacy as dignity* dovrebbe rappresentare ancora il modello di tutela per questi due rapporti (*stakeholder* e *data subject*; *stakeholder* e *data holder*): la vita privata deve essere sottratta dalla sfera pubblica salvo regole particolari poste con il rispetto di rigorose garanzie a tutela dell'individuo.

Una categoria di problemi diversa è quella che riguarda il rapporto giuridico tra *data subject* e *data holder*

[138] Neil M. Richards, *The limits of tort privacy*, cit., 2011, p. 378.

entro una cornice di confidenzialità e nel rispetto dell'identità contestuale.

Il *data sharing* sempre più massiccio vede prevalere, più che un tema di libertà, un tema di identità, un tema cioè di controllo delle informazioni in un contesto relazionale (*data subject* e *data holder*) – e non certo *erga omnes* - in cui la particolare qualità dell'informazione (personale) determina uno statuto di accessibilità limitata della stessa informazione che deve essere garantito dal *data holder*. Il fuoco della normativa è la trasparenza del *data holder* e il rispetto della confidenzialità, ossia dell'uso dei dati solo per il raggiungimento di una finalità resa palese, cioè trasparente. Il problema vero della normativa diviene quindi l'opacità del *data holder*.

Si tratta di rapporti speculari: nella *hard privacy* il valore è l'opacità e il problema è la trasparenza; nella *soft privacy* il valore è la trasparenza ed il problema è l'opacità.

Al di fuori del contesto relazionale sopra richiamato, resta la dicotomia privato/pubblico e la tutela della libertà in senso negativo (*privacy as intimacy*).

Questo modello di tutela diventa chiaramente sovrapponibile a quello del Global Privacy Standard. La confidenzialità, implicando un dovere di garantire la riservatezza (inaccessibilità) di determinate informazioni nell'ambito di determinati rapporti, rappresenta in maniera chiara la necessità che il confidente utilizzi le informazioni solo per fini che sono appropriati al contesto in cui le riceve (si pensi, ad esempio, a un avvocato). È il principio di limitazione. Per questa ragione, poi, su di lui grava il dovere di impedire l'accesso a tali informazioni da parte di soggetti non autorizzati (*data security*). Accanto a rapporti tradizionalmente ancorati a questo principio, come quello tra medico e paziente, vi sono altri rapporti in cui questa

tradizione non c'è e che richiedono quindi una preventiva informativa resa al *data subject*. È il principio di trasparenza.

Questo è il profilo statico del rapporto tra *data subject* e *data holder*, ossia quello di raccolta e memorizzazione delle informazioni. Esiste poi anche un profilo dinamico di uso delle informazioni: la norma sociale e giuridica di appropriatezza contestuale diventa centrale per garantire il rispetto della privacy identità. L'uso che potrò fare di quei dati sarà legittimo fintantoché si rispetterà il contesto, sincronico e diacronico, in cui è avvenuto lo scambio di dati. L'avvocato potrà comunicare le informazioni al suo consulente, ad esempio al medico legale, sempre nel rispetto dell'obbligo di confidenzialità, ossia con l'unica finalità di garantire la miglior tutela degli interessi del proprio assistito.

Il modello di tutela che ne emerge è quello della *privacy as contextual identity*. Come posso garantire l'identità contestuale? Anzitutto chiarendo, laddove non fosse evidente, il perimetro relazionale entro cui avviene lo scambio di informazioni. Il *data holder* raccoglie e processa informazioni dovendo rispettare i principi della *data protection*, ossia limitazione, trasparenza, base legale e *data security*. Questi principi, però, devono essere coerenti a loro volta con il principio di identità contestuale.

È del tutto superfluo richiedere il consenso per l'uso dei *cookies* quando questi garantiscono la funzionalità del servizio che l'utente sta utilizzando. Quando i medesimi *cookies*[139] consentono il tracciamento degli utenti durante la navigazione in rete e la creazione di profili che sono utilizzati per messaggi pubblicitari personalizzati, tale

[139] Nissenbaum, *Privacy as Contextual Integrity*, cit., p. 105.

attività deve essere trasparente e deve corrispondere, quanto meno, a un legittimo interesse del *data holder* (principio di base legale). Si pensi al caso in cui il servizio offerto è gratuito e la pubblicità rappresenta il modello di business sottostante. È chiaro che ci troviamo di fronte ad un legittimo interesse del *data holder* ed è altrettanto chiaro che, se tale attività è trasparente, tale attività deve essere considerata lecita. È noto come in Europa si preferisca, quale base legale del trattamento, il consenso[140]: proprio qui il principio di identità contestuale dovrebbe essere sufficiente per dirimere la questione: se per l'utente è chiaro che il contesto è di tipo commerciale e che quel determinato sito realizza i propri profitti tramite la pubblicità garantita dal *tracking*, non si realizza alcuna violazione. Vi è chiaramente una violazione nel momento in cui questi dati sono ceduti a terzi e quindi sono decontestualizzati.

Ciò che rileva, quindi, è sempre il rapporto tra *data holder* e *data subject* e il perimetro relazionale che si viene a creare. La disciplina sulla *data protection* nasceva per impedire l'esistenza di banche dati segrete e l'uso secondario dei dati raccolti[141]. E il rispetto della *digital privacy*, quarant'anni dopo, passa attraverso la realizzazione di questi stessi obiettivi.

Ancora una volta possiamo cogliere la differenza che intercorre tra *hard privacy* e *soft privacy*. Si ricorderà che Warren e Brandeis fecero ricorso a un diritto individuale e generale proprio perché il problema che loro volevano affrontare (la divulgazione di informazioni private attraverso i mass media) non poggiava su alcuna relazione

[140] Direttiva 2009/136/CE.
[141] Daniel J. Solove, *A Taxonomy of Privacy*, cit., p. 518.

giuridica. La relazione tra *data holder* e *data subject*, invece, si deve improntare essenzialmente sul rispetto di un dovere di confidenzialità, ossia sull'ossequio dei principi che abbiamo più volte evidenziato: principio di limitazione preventivo e successivo (raccolta e conservazione dei soli dati necessari al raggiungimento della finalità del trattamento); principio di trasparenza preventivo e successivo (chiarimento in un'informativa sulle modalità di questo trattamento e permesso all'interessato di accedere ai propri dati); principio di base legale (se non c'è una legge a consentire la raccolta di questi dati, è necessario che vi sia un legittimo interesse del *data holder*, una richiesta dell'interessato e, in mancanza di tutto ciò, occorrerà richiedere il consenso dell'interessato); il principio di *data security* (si deve ridurre il rischio di perdita e di accesso non autorizzato ai dati). Questi principi devono essere letti alla luce del concetto di identità contestuale che riesce a delineare ciò che è una violazione della privacy in senso positivo (identità) e ciò che invece non lo è.

La tesi che qui si intende sostenere è che la normativa sulla protezione dei dati personali ha posto implicitamente un dovere di confidenzialità in tutti i rapporti tra *data holder* e *data subject*. Tale dovere era funzionale a impedire che l'estrema velocità con cui le informazioni circolavano potesse provocare dei pregiudizi agli individui, principalmente consistenti nella decontestualizzazione delle informazioni raccolte. Il nucleo centrale è quello dell'identità contestuale: fintantoché le informazioni personali restano nel perimetro contestuale in cui sono state raccolte non vi è alcun problema; quando queste informazioni sono utilizzate fuori contesto, allora possono porsi delle criticità. Si è detto che il dovere di confidenzialità è implicito perché non si è mai

fatto riferimento a questo istituto giuridico, prediligendo un riferimento ai valori della riservatezza e dell'identità personale.

Lo scopo della normativa è far rispettare una ragionevole aspettativa che le informazioni che vengono scambiate non siano utilizzare al di fuori del loro contesto e ciò a prescindere da qualsiasi accordo contrattuale sottostante; ciò è esattamente quel che avviene in materia di confidenzialità. Per questo si vuole sostenere che, più che fare riferimento al termine privacy, appare più corretto specificare che qualsiasi trattamento di dati personali implica un obbligo di confidenzialità che si basa sui quattro principi che abbiamo richiamato; metodo adatto a risolvere anche casi limite, dai contorni più sfumati.

Se il nucleo della tutela è l'identità contestuale, gli strumenti che consentono di gestire questa identità (le *privacy enhancing technologies*) costituiscono l'altro elemento fondamentale della regolamentazione. La tutela dell'anonimato e dello pseudonimo, gli strumenti di monitoraggio delle informazioni cedute e di rimozione di quelle pregiudizievoli, rappresentano l'altra faccia della stessa medaglia.

Privacy enhancing technologies e confidenzialità si compenetrano e rendono chiaro che il primo livello di tutela è quello del perimetro in cui lo scambio di informazioni è avvenuto. Come anticipato, non esistono solo contesti privati e pubblici; esistono anche e soprattutto zone grigie in cui tale confine deve essere disegnato da norme sociali e giuridiche, la cui formulazione emerge grazie all'esperienza e all'uso di tecnologie nuove. Se si fuoriesce da tale cornice e, quindi, si concretizza una violazione dell'identità contestuale di un soggetto, il responsabile principale è il *data holder* che abbia violato questo dovere di confidenzialità, in base al quale era

vincolato a rispettare regole precise nella raccolta e nell'utilizzo dei dati (*information collection* e *information processing*).

4. Conclusioni.

Questa tesi ha raggiunto tre conclusioni fondamentali in relazione a: concetto di privacy, fuoco normativo della *data protection*, nuova tassonomia riguardante le violazioni in materia di privacy.

L'analisi dei valori e dei modelli di tutela evidenzia, in primo luogo, il significato complesso e multiforme della parola "privacy". Privato è lo stato o la qualità di una certa cosa che non è generalmente accessibile. Il suo significato si arricchisce in contrapposizione al concetto di pubblico. Pubblico sta sia per quello che è generalmente accessibile alla collettività, sia per quello che riguarda tale collettività, sia, ancora, per quello che si riferisce alla collettività nella sua articolazione istituzionale che chiamiamo Stato-apparato, confondendolo spesso con lo Stato-comunità. Lo statuto di limitata accessibilità di un'informazione non riguarda solo la dicotomia pubblico/privato ma può dipendere anche dalla qualità dell'informazione (il segreto di Stato) e il rapporto che lega due soggetti (l'obbligo di confidenzialità del medico). Le violazioni della privacy possono allora concernere sia la diffusione di fatti privati in pubblico (privacy orizzontale), sia le garanzie costituzionali contro l'invasione di spazi privati (privacy verticale), sia la violazione degli obblighi del *data holder* (*data protection*). Molteplici angolazioni di un problema comune.

In secondo luogo, il Global Privacy Standard (o GPS) propriamente detto riguarda una serie di principi procedurali che fissano il corretto trattamento delle informazioni personali (*Fair Information Practices*, com'è definito il Global Privacy Standard in ambito statunitense). Il centro della normazione è la relazione qualificata tra

data subject e *data holder*. Qualificata perché riteniamo che il trattamento di dati personali implichi un dovere di confidenzialità, cioè una nuova forma di confidenzialità che fornisce forma giuridica al contesto relazionale entro cui avviene lo scambio di informazioni. Il principio fondamentale è il principio di trasparenza: prima dell'inizio del trattamento e successivamente, quando il *data holder* deve consentire, attraverso strumenti specifici (anonimizzazione, rimozione, segnalazioni di abusi, adesione a procedure di risoluzione delle controversie), a rimodulare l'identità contestuale del *data subject*.

In terzo e ultimo luogo abbiamo quindi proposto una classificazione delle possibili violazioni in materia di privacy a partire dai possibili rapporti giuridici rilevanti. A tal fine abbiamo introdotto la figura di un portatore di interessi (*stakeholder*) in contrasto con quelli all'inaccessibilità dell'informazione. Pertanto, quando non è riscontrabile una relazione qualificata tra *data subject* e *data holder*, vi sono due altre ipotesi: un rapporto tra *stakeholder* e *data subject* e tra *stakeholder* e *data holder*. Nel primo caso, abbiamo verificato che vi è un modello di tutela caratterizzato da una regola generale - prevalenza dell'interesse privato - e da una regola particolare - prevalenza dell'interesse pubblico, declinato attraverso una serie di garanzie in caso di privacy verticale e attraverso un paramento di essenzialità in caso di privacy orizzontale. Nel secondo caso, si dovrebbero applicare le stesse garanzie e gli stessi principi; queste garanzie e questi principi delineano la quota di libertà (negativa) presente in un certo ordinamento. Trattandosi di questioni fortemente connotate da un punto di vista politico, queste ipotesi non sono facilmente inquadrabili in un Global Privacy Standard, ossia in un accordo transnazionale.

Bibliografia.

Alessandro Acquisti, *Privacy*, in *Rivista di Politica Economica*, 2005.
Alessandro Acquisti, Leslie John e George Loewenstein, *What is privacy worth?*, in *Twenty First Workshop on Information Systems and Economics* (WISE), 2009.
Alessandro Acquisti, *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publication, 2007.
Analysis Of Antiterrorism Data Mining, in *Boston College Law* Review, 2007.
Norberto Nuno Gomes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and articulating Rights*, in AAVV, *Privacy and identity management for life*, Springer, 2010.
Hannah Arendt, *Vita Activa*, Milano, 2009.
Lisa Austin, *Privacy and the Question of Technology*, in *Law and Philosophy*, 2003.
Zygmunt Bauman, *Modernità Liquida*, Bari, 2011.
Isaiah Berlin, *Libertà*, Milano2010.
Cesare Massimo Bianca (a cura di), *La Protezione dei dati personali*, Padova, 2007.
Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining,* in *Boston College Law Review,* 2007.
Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, in *Computer Law & Security Report*, 2008.
Asa Briggs e Peter Burke, *Storia sociale dei media*, Bologna, 2010.
Norberto Bobbio, *Eguaglianza e libertà*, Torino, 1995.
Norberto Bobbio, *Introduzione alla filosofia del diritto*, Torino, 1948.

David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*, 1998.
Dan Burk, *Privacy and Property in the Global Datasphere*, in *Minnesota Legal Studies Research Paper*, 2007.
Debora Caldirola, *Il diritto alla riservatezza*, Padova, 2006.
Eva Cantarella, *Itaca - Eroi, donne, potere tra vendetta e diritto*, Milano, 2008.
Manuel Castells, *Galassia internet*, Milano, 2006.
Fred H. Cate, Robert E. Litan, *Constitutional Issues in Information Privacy*, in *Michigan Law Review*, 2002.
F. Di Ciommo, Giappichelli, *Diritti della personalità tra media tradizionale e avvento di Internet*, Torino, 2003.
Citron, Danielle Keats and Henry, Leslie Meltzer, *Visionary Pragmatism and the Value of Privacy in the Twenty- First Century*, in *Michigan Law Review*, 2010.
Julie E. Cohen, *Privacy, Visibility, Transparency and Exposure*, in *University of Chicago Law Review*, 2008.
Jean Cohen, *Regulating Intimacy: A New Legal Paradigm*, Princeton, 2002.
Julie E. Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice*, in *Yale University Press*, 2012.
Alessandra Facchi, *Breve storia dei diritti umani*, Bologna, 2007.
Vittorio Fanchiotti, *U.S. v. Jones: una soluzione tradizionalista per il futuro della privacy?*, in *Diritto penale e processo*, 2012.
Maria Rosaria Ferrarese, *Prima lezione di diritto globale*, Bari, 2012.
Stefano Ferrucci, *L'oikos nelle leggi della polis. Il privato ateniese tra diritto e società*, in *Etica & Politica*, 2007.

Giusella Finocchiaro (a cura di), *Diritto all'anonimato: anonimato, nome e identità personale*, Padova, 2008.
Gianluigi Fioriglio, *Il diritto alla privacy: nuove frontiere nell'era di internet*, Bologna, 2008.
David H. Flaherty, *Governmental Surveillance and Bureaucratic Accountability: Data Protection Agencies in Western Societies*, in *Science, Technology & Human Values*, 1986.
Luciano Floridi, *The ontological interpretation of informational privacy*, Springer, 2006.
Charles Fried, Privacy, Yale Law Journal, 1968.
David Friedman, *L'ordine del diritto*, Bologna, 2004.
Vittorio Frosini, *L'ipotesi robinsoniana e l'individuo come ordinamento giuridico*, in *Sociologia del diritto*, 2001.
Amy Gajda, *What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering The Press Coverage That Led to The Right to Privacy*, in *Illinois Public Law and Legal Theory Research Papers Series*, 2007.
Francesco Galgano, *Lex mercatoria*, Bologna, 1993.
Alan E. Garfieldt, *Promises of Silence: Contract Law and Freedom of Speech*, in *Cornell Law* Review, 1998.
Giulio Garuti, *Intercettazioni telefoniche e politica in Lituania,* in *Diritto Penale e Processo*, 2012.
James Gleick, *L'informazione. Una storia. Una teoria. Un diluvio*, Milano, 2012.
James Grimmelmann, *Saving Facebook*, in *Iowa Law Review*, 2009.
Marit Hansen, *Marrying Transaprency Tools with User-Controlled Identity Management*, in *AAVV IFIP International Federation for Information Processing; The Future of Identity in the Information Society*, Springer, 2008.
Geoffrey C. Hazard e Angelo Dondi, *Etiche della professionale legale*, Bologna, 2005.

Fischer Simone Hubner e AA.VV., *Privacy and Identity Management for Life*, Helsinborg, 2010.
Henry Laborit, *La vita anteriore*, Mondadori, Milano, 1990.
Lawrence Lessig, *Cultura libera*, Milano, 2005.
Lawrence Lessig, *Privacy as property*, in *Social reserch*, 2002.
David Lyon, *La società sorvegliata tecnologie di controllo della vita quotidiana*, Milano, 2003.
Maria Rosaria Marella, *Oltre il pubblico e il privato*, Perugia, 2012.
Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality*, in *Univeristy of Cincinnati Law Review*, 2006.
Thomas Nagel, *Concealment And Exposure*, in *Oxford University Press*, 2002.
Ugo Mattei, *Beni comuni. Un manifesto*, Bari, 2011.
Helen Nissenbaum, *Privacy as contextual integrity*, in *Washington Law Review*, 2004.
Helen Nissenbaum, *Privacy in Context*, in *Stanford University*, 2009.
Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy*, in *Public, Law & Philospophy*, 1998.
Mauro Paissan (a cura di), *Privacy e giornalismo*, Roma, 2008.
John Palfrey e Urs Grasser, *Nati con la rete*, Milano, 2009.
Andreas Pfitzmann e Katrin Burcea-Pfitzmann, *Lifelong Privacy: Privacy and identity management for life,* in AA. VV., *Privacy and Identity Management for Life* Springer, 2010.
Ugo Pangallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008.

Richard A. Posner, *The Economics of Justice*, in *Harvard University*, 1981.
William Lloyd Prosser, *Privacy*, in *California Law Review*, 1960.
John Rawls, *Lezioni di storia della filosofia politica*, Milano, 2009.
Neil M., Richards, *Intellectual Privacy*, in *Texas Law Review*, 2008.
Neil M. Richards, *The Limits Of Tort Privacy*, in *Journal on Telecomunication and High Tech Law,* 2011.
Neil Richards, *The informational privacy law project*, in *Georgetown Law Journal*, 2006.
Neil Richards, Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, in *Georgetown Law Journal*, 2007.
Neil M. Richards e Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, in *California Law Review*, 2010.
Stefano Rodotà, *Data Protection as a fundamental right,* in *Reinventing data protection*, Springer, 2009.
Stefano Rodotà, *La vita e le regole*, Milano, 2009.
Guido Rossi, *Il gioco delle regole*, Milano, 2006.
Gavison Ruth, *Privacy and the Limits of Law*, in *Yale Law Journal*, 1980.
Viktor Mayer Schönberger, *Delete: il diritto all'oblio nell'era digitale*, Milano, 2010.
Thomas J. Smedinghoff, *It's All About Trust: The Expanding Scope of Security Obligations in Global Privacy and E-Transactions Law*, in *Michigan State University College of Law Journal of International Law*, 2007.
Wolfgang Sofsky, *In difesa del privato*, Torino, 2007.
Daniel J. Solove, *The Digital Person - Technology And Privacy In The Information Age*, in *New York University Press*, 2004.

Daniel J. Solove, *Nothing to Hide - The False Tradeoff between Privacy and Security*, *Yale University Press*, 2011.
Daniel J. Solove, *Conceptualizing Privacy*, in *California Law Review*, 2002.
Daniel J. Solove, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review*, 2006.
Daniel J. Solove, *No privacy*, Milano, 2009.
Daniel J. Solove, *Understanding Privacy*, in *Harvard University Press*, 2008.
Daniel J. Solove e Chris Jay Hoofnagel, *A Model Regime Of Privacy Protection*, in *University of Illinois Law Review*, 2006.
Lior Strahilevitz, *A Social Networks Theory of Privacy*, in *University of Chicago Law School*, 2004.
Aljs Vignudelli, *Diritto costituzionale*, Torino, 2010.
Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You*, in *Stanford Law Review*, 2000.
Tim Wafa, *Global Internet Privacy Rights: A Pragmatic Approach*, in *University of San Francisco Intellectual Property Law Bulletin*, 2009.
Yang Wang e Alfred Kobsa, *Privacy-Enhancing Technologies*, in *Handbook of Research on Social and Organizational Liabilities in Information Security*, Hershey, IGI Global, 2009.
Samuel Warren and Louis Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890.
Alan Westin, *Privacy and Freedom*, in *New York: Athenum*, 1967.
Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, in *Rutgers Law Journal*, 2002.

Gustavo Zagrebelsky, *Intorno alla legge. Il diritto come dimensione del vivere comune*, Torino, 2009.
Jonathan Zittrain*, The future of the Internet and how to stop it, Yale University Press*, 2000.