UNIVERSITY
OF TRENTO - Italy
Faculty of Law
Department of Legal Sciences

lawtech

Trento Law and Technology
Research Group
Student Paper n. 35

LA PRIVACY BY DESIGN: UN'ANALISI COMPARATA NELL'ERA DIGITALE

GIORGIA BINCOLETTO

ISBN: 978-88-8443-733-4

KEYWORDS

Law of the Digital Age – Privacy – Data Protection – Privacy by Design – Comparative Law

About the author

Giorgia Bincoletto (giorgia.binco@gmail.com) graduated in Law, *magna cum laude,* at the University of Trento, under the supervision of Prof. Roberto Caso and Dr. Paolo Guarda (March 2017).

The opinion stated in this paper and all possible errors are the Author's only.

PAROLE CHIAVE

Diritto dell'era digitale – Privacy – Protezione dei dati personali – Privacy by Design – Diritto comparato

Informazioni sull'autore

Giorgia Bincoletto (giorgia.binco@gmail.com) ha conseguito la Laurea in Giurisprudenza, *magna cum laude,* presso l'Università di Trento con la supervisione del Prof. Roberto Caso e del Prof. Paolo Guarda (March 2017).

Le opinioni e gli eventuali errori contenuti sono ascrivibili esclusivamente all'autore.

Abstract

The Digital Age brings along some relevant changes for lawyers and jurists. As a matter of fact, modern technologies invention and their diffusion cause specific requirements in order to protect the right of privacy because of the huge collection of individual's information. Today, the concept of privacy is changing: the right to be let alone evolves in personal data protection.

The aim of this thesis is to propose and explain the innovative approach of privacy by design. This new methodology for privacy protection may be an efficient solution for technologies challenges and may increase law enforcement. The starting point is certainly the law and his power to conform technology with the regulative system.

Privacy by design approach has as a goal to design and develop a system, a product or a service in a way that supports and materializes privacy principles, rules and values. Privacy measures are embedded into the design and the architecture of ICT systems and business practices. Privacy by design is characterized by proactive technical and organizational measures in time for preventing privacy infractions in each situation and for better safeguarding data collection and data security. The concept requires more respect for user privacy, keeping it central.

The idea of privacy by design arose in Canada thanks to the Commissioner Ann Cavoukian and then became an international principle for privacy protection. It is even used by Federal Trade Commission and Canadians Commissioners in few procedures. Nowadays some norms explicitly require privacy by design; this is the case of the General Data Protection Regulation of the European Union published in 2016.

The main goal of this work is to analyze the principle in a critical, comparative and interdisciplinary way, considering the historical point of view, the regulatory interventions and the case law. The analysis might be useful for understanding and implementing the approach in more countries, taking into account the benefits and the level of criticality. It is necessary to give some guidelines for the real implementation of privacy by design, looking at the future, and to find a norm that can be applied all over the word; in fact, it is urgent to find a global solution for privacy concerns.

Privacy by design won't be the unique solution for privacy protection, but it will be essential for his future. This principle will safeguard better individual rights through a coherent and whole method. Designing privacy-friendly the technology means guarantee the other fundamental rights even more.

Abstract

L'era digitale porta con sé una serie di cambiamenti rilevanti per il mondo giuridico. La necessità della tutela della privacy è una conseguenza diretta dell'invenzione e della diffusione di strumenti tecnologici che consentono di carpire quante più informazioni possibili dell'individuo. Oggi si assiste all'evoluzione della tutela e del concetto di riservatezza: dall'individuo che vuole essere lasciato solo, alla protezione dei dati personali e della loro circolazione.

Nella presente tesi si intende proporre una soluzione che sappia rispondere al meglio alle sfide lanciate dalle nuove tecnologie e potenziare l'efficienza delle norme giuridiche: l'approccio innovativo di privacy by design. Questo principio impone l'incorporazione delle regole e dei valori della privacy fin dalla progettazione dei prodotti e dei servizi. Il concetto aspira a ridefinire la privacy, per tutelare la riservatezza e i dati personali *ex ante,* con misure tecniche e organizzative che siano adeguate al caso concreto, che garantiscano una maggior sicurezza e una miglior garanzia della raccolta e del trattamento e considerino al centro l'utente/consumatore. Il punto di partenza e di arrivo è sempre il diritto e il suo potere di conformare la tecnologia alle sue regole.

La privacy by design nasce come elaborazione dottrinale, per poi affermarsi a livello internazionale come principio, essere inserita a livello normativo in varie fonti, nella prassi della Federal Trade Commission e delle Autorità Canadesi ed essere infine codificata nel nuovo Regolamento Europeo sulla Protezione dei Dati dell'aprile 2016.

Si intende approfondire il principio attraverso un'analisi critica e comparata e un approccio interdisciplinare, che tenga conto della sua elaborazione storica, normativa e giurisprudenziale. L'obiettivo è presentare un quadro completo di ricostruzione, che possa risultare utile per una sua comprensione ed applicazione concreta in più ordinamenti giuridici. Verranno delineati anche i vantaggi e gli aspetti che contraddistinguono la privacy by design, sottolineandone alcuni profili critici, e verranno proposte delle linee guida da seguire per adottare il principio e delle esemplificazioni, con uno sguardo al futuro. Si aspira all'elaborazione di una norma sulla privacy by design condivisa e condivisibile grazie alla diffusione delle scelte operative in ambito interno e internazionale: nell'era digitale c'è urgenza di assicurare un'effettiva e maggiore protezione dei dati personali a livello mondiale.

La privacy by design non potrà essere una soluzione tutti i possibili trattamenti di dati personali, ma può essere presentata come il futuro della loro protezione. È un approccio globale che comporta una maggiore tutela dei diritti dei cittadini, in modo coerente e completo. Progettare le tecnologie in modo privacy-friendly è doveroso non solo per proteggere la riservatezza e i dati degli individui, ma anche per garantire che l'esercizio degli altri diritti fondamentali non sia ingiustamente penalizzato.

Indice

Introduzione

"Anche se è eccessivo, e persino pericoloso dire che noi siamo i nostri dati, è tuttavia vero che la nostra rappresentazione sociale è sempre più affidata a informazioni sparse in una molteplicità di banche dati, e ai profili che su questa base vengono costruiti, alle simulazioni che permettono. Siamo sempre più conosciuti da soggetti pubblici e privati attraverso i dati che ci riguardano, in forme che possono incidere sull'eguaglianza, sulla libertà di comunicazione, di espressione o di circolazione, sul diritto alla salute, sulla condizione di lavoratore, sull'accesso al credito e alle assicurazioni, e via elencando. Divenute entità disincarnate, le persone hanno sempre di più bisogno di una tutela del loro corpo elettronico".

Rodotà, Il diritto di avere diritti, 2012.

L'era digitale porta con sé una serie di cambiamenti rilevanti per il mondo giuridico. Per risolvere i nuovi problemi possono essere escogitate più soluzioni, tenendo conto del peculiare rapporto tra il diritto e la tecnologia. La regola può essere imposta dal legislatore o essere incorporata direttamente nello strumento tecnologico: il codice informatico assume un ruolo fondamentale.

Il problema della tutela della privacy è una conseguenza diretta dell'invenzione e della diffusione di tecnologie che consentono di carpire quante più informazioni possibili dell'individuo. Dalla prima fotocamera della Kodak, al più sofisticato algoritmo di Google, l'aspirazione personale dei soggetti rimane quella di proteggere la sfera privata della propria vita.

Oggi, nella società dominata dall'informatica, si assiste all'evoluzione della tutela e del concetto di riservatezza: dall'individuo che vuole essere lasciato solo, alla protezione dei dati personali e della loro circolazione.

Nella presente tesi si intende proporre una soluzione che sappia rispondere al meglio alle sfide lanciate dalle nuove tecnologie: l'approccio innovativo di privacy by design. Questo principio impone l'incorporazione delle regole e dei valori della privacy fin dalla progettazione dei prodotti e dei servizi.

Il concetto aspira a ridefinire la privacy, per tutelare la riservatezza e i dati personali *ex ante,* con misure tecniche e organizzative che siano adeguate al caso concreto. Privacy by design significa una maggior sicurezza dei dati personali e una miglior garanzia della raccolta e del trattamento del minor numero di dati possibile. L'utente e il consumatore sono considerati al centro e la progettazione delle soluzioni tecniche tiene conto fin dall'origine delle regole e dei principi imposti dal diritto.

La privacy by design nasce come elaborazione dottrinale, per poi affermarsi a livello internazionale ed essere infine codificata nel nuovo Regolamento Europeo sulla Protezione dei Dati dell'aprile 2016.

Si intende approfondire il principio attraverso un'analisi critica e comparata, che tenga conto della sua elaborazione storica, normativa e giurisprudenziale. L'obiettivo è presentare un quadro completo di ricostruzione, che possa risultare utile per una sua comprensione ed applicazione concreta in più ordinamenti giuridici.

Per questo lavoro è stato fondamentale un approccio basato sull'interdisciplinarietà, per aprire al dialogo tra i giuristi, gli informatici, gli ingegneri, gli economisti e in generale tutte le figure professionali coinvolte. È impensabile affrontare il problema della tutela della privacy nell'era digitale soltanto dal punto di vista giuridico, senza considerare gli altri interessi e le altre dinamiche presenti. La realtà è ricca di sfaccettature particolareggiate, inevitabilmente non incasellabili in un unico sapere.

Inoltre, è stato necessario utilizzare un approccio comparatistico, dal momento che i fenomeni giuridici sorpassano i confini ideali degli Stati.

La trattazione dell'argomento si articola come segue.

Il primo capitolo affronta delle questioni preliminari per contestualizzare il principio nell'era del Web 2.0. Innanzitutto, viene analizzato lo stretto legame tra il diritto e la tecnologia e i cambiamenti che questa ha portato nel panorama giuridico. Si spiegherà perché si ritiene auspicabile adottare una visione integrata tra i diversi tipi di professionalità: informatica, giuridica, organizzativa. Verrà tracciata brevemente la nascita e l'evoluzione della tutela della privacy e si analizzerà nel dettaglio la definizione di dato personale, per chiarire l'oggetto della tutela. In seguito, si approfondirà la stretta relazione tra privacy e sicurezza, per presentare il contesto in cui può utilmente inserirsi il principio.

Il secondo capitolo traccia il processo ventennale di elaborazione della privacy by design che ha avuto inizio negli anni novanta in Canada e che oggi ha condotto ad una sua formulazione positiva nella legislazione europea. Si intende mostrare come la riflessione si sia trasferita da un livello dottrinale e programmatico ad un piano organizzativo e legislativo in vari ordinamenti giuridici. Verranno presentati i momenti chiave del principio, dalla Resolution of Jerusalem, al Report della Federal Trade Commission degli Stati Uniti e alla Proposta di regolamento della Commissione Europea. Si esaminerà l'articolo 25 del Regolamento Europeo sulla Protezione dei Dati del 2016, il quale impone al titolare del trattamento dei dati di adottare la privacy by design attraverso la predisposizione di misure tecniche ed organizzative. Compiendo poi un'analisi storica e interpretativa si dimostrerà che si possono rilevare delle tracce del principio già in precedenti norme europee ed italiane e in documentazioni di soft law provenienti dalle autorità garanti della privacy o dalla stessa Commissione Europea.

Successivamente, si intende delineare in modo approfondito quali siano i vantaggi e gli aspetti che contraddistinguono l'oggetto della presente tesi, attraverso vari contributi dottrinari provenienti soprattutto da oltreoceano e

appartenenti a giuristi, economisti, ingegneri e ad informatici. Non verranno poi nascosti alcuni profili critici che ad oggi impediscono una diffusione capillare dell'approccio, cercando di argomentare la loro superabilità. Per concludere la trattazione centrale si proporranno delle linee guida da seguire per l'auspicabile adozione giuridica della privacy by design, con uno sguardo al futuro.

Il terzo capitolo presenta le esperienze canadesi e statunitensi per approfondire l'argomento in prospettiva comparatistica ed evidenziare le norme che oggi richiamano il principio al di là dell'oceano. Verrà anche proposto un prototipo di norma sulla privacy by design per fornire un parametro di confronto con il citato articolo 25 e un modello per l'introduzione legislativa del principio nei due ordinamenti di common law, in cui in cui vengono condensate tutte le riflessioni teoriche esposte nei precedenti capitoli.

La parte conclusiva dell'opera riporta alcune esperienze che hanno già implementato la privacy by design in alcuni ambiti giuridici, dimostrando che l'incorporazione della regola giuridica nello strumento tecnologico è non solo una possibilità concretizzabile, ma anche una soluzione efficace che non sacrifica l'innovazione e la creatività della scienza. Verrà infine descritto un modello certificatorio da poco attivo in Canada e contraddistinto dal marchio "*privacy certified by design*".

Capitolo 1: La Privacy 2.0

"Così molti giuristi vivono l'innovazione tecnologica
come un'espropriazione continua,
non come
un terreno nuovo in cui cimentarsi"
Rodotà, Il diritto di avere diritti, 2012.

1. Diritto e Tecnologia: la *lex informatica*

La rivoluzione tecnologica e quella telematica hanno comportato delle profonde conseguenze per il mondo del diritto.

In alcuni casi il diritto ha tentato di utilizzare le norme esistenti senza adattarsi alle novità delle tecnologie, in altri ha "abdicato" alla sua regolamentazione, lasciando alla tecnologia il compito di dare la regola al caso concreto[1]. Solo più tardi, il diritto ha ripreso il suo ruolo regolatore e ha provveduto a disciplinare i vari fenomeni sempre nuovi e sempre più difficili da affrontare.

Tutto ciò ha creato delle ripercussioni inevitabili sul sistema delle fonti, sulla certezza e sull'efficacia del diritto, non più legato strettamente al carattere statuale e così anche sul fondante principio di legalità.

In concreto, la realtà giuridica è cambiata e con essa sono mutate le concezioni di spazio[2], di proprietà[3], di libertà[4], di contratto[5], di documento[6] e

---

[1] Si veda il contributo di G. PELLEGRINO, *I rischi del diritto nella Rete globale*, in *Informatica dir.*, 2009, fasc. 1, 256.

[2] Un'analisi attenta si trova in V. DE ROSA, *La formazione di regole giuridiche per Il "Cyberspazio"*, in *Dir. informazione e informatica*, 2003, fasc. 2, 361-362: *"Con lo sviluppo dell'"Information Technology" si è venuto a creare un nuovo spazio, o, se si preferisce, una nuova dimensione spaziale nell'ambito della quale viene ad esplicarsi l'attività umana in tutte le sue manifestazioni e rispetto al quale il medium informatico costituisce un organon, vale a dire uno strumento di percezione e, al tempo stesso, di creazione dello spazio medesimo; costituito dalle interazioni che vengono a stabilirsi tra le intelligenze artificiali create per effetto dei sistemi informatici (il cui studio forma oggetto specifico della cibernetica) nonché dalle relazioni che vengono a stabilirsi all'interno di esso: ciò che si suole denominare cyberspazio*".

[3] Si veda come esempio di nuovo paradigma proprietario, S. MONTALDO, *Internet e Commons: le risorse della rete nella prospettiva dei beni comuni*, in *Dir. informazione e informatica*, 2013, fasc.2, 287-306.

[4] Si veda, per una riflessione sulle nuove libertà, anche politiche, M. CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Dir. informazione informatica*, 2015, fasc. 2, 275-314.

[5] Si vedano due interessanti contributi sui contratti conclusi via Internet, C. ROSSELLO, *Commercio Elettronico: la governance di internet tra diritto statuale, autodisciplina, soft law e lex mercatoria*, Giuffrè, Milano, 2006; G. FINOCCHIARO, *Lex mercatoria e commercio elettronico, il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, 2001, fasc. 2, 573: "*il problema dell'individuazione della legge applicabile agli atti compiuti via Internet è un problema di carattere generale, ed è anzi il problema di maggior rilievo che, fra le questioni sollevate dalla grande rete, si pone oggi al giurista".*

altre ancora. Lo spazio telematico, ad esempio, è un "*non-luogo, poiché i luoghi appartengono a terra mare aria*"[7]. La mancanza della dimensione spaziale ha un impatto decisivo sull'individuazione del diritto da applicare, diritto che deve essere adeguato o creato con nuovi criteri e differenti presupposti.

Internet, la Rete, è così un mondo a sé stante, contraddistinto dai propri e diversi problemi giuridici, la cui soluzione va cercata in dialogo tra diritto e tecnologia. Anche chi non condivide la visione dell'esistenza di una realtà separata, ritenendo che si tratti unicamente della comparsa di un nuovo mezzo di comunicazione[8], accessibile a tutti da ogni parte del globo, non nasconde che le peculiarità del mezzo meritano un'analisi giuridica attenta.

Da un punto di vista filosofico grandi giuristi si sono occupati della relazione tra diritto e tecnica, intesa come artificialità, come una manipolazione della natura. Si è scritto che "*la tecnica non si lascia ridurre a semplice strumento, a qualcosa che l'uomo sceglie, adopera, e poi mette da canto. Essa penetra nella quotidianità*"[9]. Come afferma l'autore citato, il giurista deve prendere posizione, compiere delle scelte e ritagliarsi il suo ruolo, membro di una generazione dissimile da quella conosciuta nel passato.

È doveroso, però, ricordare che il vero compito del diritto non è solo di creare regole, ma anche di determinarne lo scopo, dato che la tecnica, lasciata sola, incapace per sua natura, non può racchiuderlo; infatti la definizione del fine è la tipica capacità del diritto, benché possa risultare spesso *"indebolito dinanzi alla potenza della tecnica"*[10]. Il valore e lo scopo della norma giuridica sono prerogativa della politica e così del potere democratico. La tecnica in questo non può influire e non influirà.

Il diritto, in realtà, è sempre stato in relazione con la tecnologia, già a partire dall'invenzione della scrittura, della penna e del linguaggio[11]. L'avvento delle tecnologie digitali rappresenta tuttavia una svolta epocale per il mondo del diritto[12]: cambiano la produzione, la rappresentazione e l'accesso alla conoscenza giuridica, l'organizzazione del lavoro e la formazione del giurista e la diffusione dei materiali giuridici. La tecnologia può influire sul contenuto delle

---

[6] Sul documento digitale è esaustivo nel capitolo ad esso dedicato G. PASCUZZI, *Il diritto dell'era digitale*, Il Mulino, Bologna, 2010, 98-122. Nella nuova edizione dell'opera del 2016 il secondo capitolo, scritto da Giovanni Pascuzzi e Paolo Guarda, è dedicato all'evoluzione del concetto di documento e sottoscrizione: G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016, 77-94.

[7] N. IRTI, *Norma e luoghi: problemi di geo-diritto*, Laterza, Bari, 2006, 61.

[8] È di questo avviso A. MANTELERO, *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, in *Contr. impr.*, 2005, fasc. 2, 659.

[9] N. IRTI, *La filosofia di una generazione*, in *Contr. impr.*, 2011, fasc. 6,1308.

[10] Un'importante riflessione sul diritto e tecnica è di L. MENGONI, *Diritto e tecnica,* in *Riv. trim. dir. proc. civ.*, 2001, fasc. 2, in commento alle parole di N. IRTI e E. SEVERINO, *Le domande del giurista e le risposte del filosofo,* in *Contr. impr.*, 2000, 665.

[11] PASCUZZI, *Il diritto dell'era digitale*, cit., 9-10. Anche nella nuova edizione si può trovare un riferimento, PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., 13-14.

[12] *Ibidem,* 33.

posizioni giuridiche tutelate, sullo scopo delle norme, sulla loro attualità e la loro formazione[13]. Gli istituti giuridici evolvono, ed è il caso del copyright, e le regole che li disciplinano devono adeguarsi alla peculiarità del mezzo tecnologico, anche con riferimento alla fonte e alla loro struttura. Secondo Giovanni Pascuzzi il diritto dell'era digitale appare deterritorializzato, destatualizzato, dematerializzato[14].

È evidente pertanto che i fenomeni giuridici dell'era informatica pongono dei problemi, nei confronti dei quali si possono escogitare più soluzioni. Al di là dell'attribuzione legislativa di regole a fenomeni giuridici, sfruttando principi e norme già poste o elaborando nuove disposizioni, si possono individuare altre forme innovative di regolazione. La regolamentazione cosiddetta dall'esterno, contraddistinta dalla definizione di parametri generali e di sanzioni, presenta infatti dei limiti, dovuti alla struttura della stessa rete[15]; perciò si potrebbe pensare di affiancarle una regolamentazione dall'interno, ponendo le regole giuridiche di pari passo con lo sviluppo della tecnologia.

Si sta così presentando la modalità di determinazione della regola attraverso la tecnica. Ci si riferisce alle norme tecniche, a quella che è stata definita la *lex informatica.* La tecnica fa diritto. Si ha una regolamentazione non diretta, non espressa, non pubblica[16]. Le regole tecniche sono un fenomeno molto diffuso nell'information society, sono il frutto della libera strutturazione dello strumento tecnologico da parte del suo artefice. Il tecnico plasma il prodotto del suo lavoro inserendo nel codice vincoli e limiti che si traducono in regole di utilizzo per l'utente, il cittadino, il consumatore.

Su questo punto non si può tralasciare l'insegnamento di Lawrence Lessing nel suo Code[17]. Il codice, a suo avviso, ha natura normativa. I bit sono i mattoni della struttura del virtuale e incorporano i valori che si intendono tutelare [18]. La modalità con cui il codice regola il cyberspazio, chi sono i soggetti coinvolti e chi li controlla, sono domande chiave per l'era digitale[19]. A questo

---

[13] *Ibidem, 261.*

[14] Professore Ordinario di Diritto Privato Comparato presso la Facoltà di Giurisprudenza di Trento.

[15] Così si legge in MANTELERO, *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, cit., 671.

[16] Sulla natura della regolamentazione dall'interno, si veda G. FINOCCHIARO, *Riflessioni su Diritto e Tecnica*, in *Dir. informazione e informatica*, 2012, fasc.4-5, 837.

[17] L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, A Member of the Perseus Books Group, New York, 1999.

[18] L. LESSIG, *Code*, version 2.0, Basic Books, A Member of the Perseus Books Group, New York, 2006, 5: "*In real space, we recognize how laws regulate—through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates—how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's "law."6 "Lex Informatica," as Joel Reidenberg first put it,7 or better, "code is law."*

[19] *Ibidem*, 79: "*How the code regulates, who the code writers are, and who controls the code writers—these are questions on which any practice of justicemust focus in the age of*

proposito, Lessing fornisce molti esempi concreti di regolazione del codice in relazione a diversi ambiti applicativi, spiegando che il diritto ha da sempre influito sulla tecnologia, su ogni fenomeno artificiale, in modo da poter conformare la realtà alle sue prescrizioni. Basti allora pensare ad un edificio pubblico e alla previsione di norme che prescrivono la costruzione di rampe di accesso per i soggetti disabili; in questa comune e semplice ipotesi il diritto ha condizionato il fenomeno artificiale nella sua struttura, nella sua realizzazione. La metafora è di aiuto: ciò che si auspica per il cyberspazio è l'incorporazione delle regole nello strumento digitale.

In un prezioso contributo d'oltreoceano, riguardante il processo di comunicazione delle informazioni digitali, viene presentato un quadro molto dettagliato sulla *lex informatica*[20]. In particolare, nell'articolo indicato si spiega che nella società dell'informazione si possono implementare due tipologie di misure, da inserire poi nella tecnologia: le regole inalterabili e le regole flessibili. La fonte di queste regole è triplice: possono essere create dalla tecnologia stessa, dal diritto che influenza la tecnologia, e dal diritto che impone all'utilizzatore di non mettere in atto certe azioni quando utilizza lo strumento informatico. La *lex informatica* viene definita come un sistema di regole parallelo per il governo delle informazioni. In aggiunta, nell'articolo si propone un confronto tra la *lex informatica* e la *legal regulation*, ossia ciò che per il nostro ordinamento è il diritto statuale.

La tabella, di cui si riporta fedelmente il contenuto[21], nello schema di seguito, è un colpo d'occhio diretto per raffrontare i due sistemi di regole.

	Legal regulation	*Lex Informatica*
Framework	*Law*	*Architecture standards*
Jurisdiction	*Physical Territory*	*Network*
Content	*Statutory Court Expression*	*Technical Capabilities, Customary Practice*
Source	*State*	*Technologists*
Customized Rules	*Contract*	*Configuration*

cyberspace. The answers reveal how cyberspace is regulated. My claim in this part of the book is that cyberspace is regulated by its code, and that the code is changing. Its regulation is its code, and its code is changing".

[20] J. R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553 (1997-1998), 568: "*Rules established in this fashion form a legal regulatory regime. In the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information. Technological architectures may prohibit certain actions on the network, such as access without security clearances, or may impose certain flows, such as mandatory address routing data for electronic messages. Technology may also offer policymakers a choice of information flow rules through configuration decisions".*

[21] *Ibidem*, table of *Features of Lex Informatica,* 569.

Customization Process	*Low Cost, Moderate cost standard form, High cost negotiation*	*Off-the-shelf Configuration, Installable Configuration, User choice*
Primary Enforcement	*Court*	*Automated, Selfexecution*

Questo schema è certamente legato al contesto statunitense, da cui proviene l'autore, ma potrebbe essere al contempo riferito al nostro ordinamento e così all'ordinamento europeo; infatti, ciò che conta sottolineare è l'approccio totalmente diverso offerto dalla *lex informatica*. Come si può notare, il quadro normativo legale è dato dal diritto e quello informatico dagli standard tecnici, la fonte diverge e il *primary enforcement* da un lato è garantito dalle varie corti e i loro giudici, dall'altro è automatico e lasciato all'auto-regolamentazione.

Un aspetto molto interessante è la giurisdizione: con la *lex informatica* si supera il concetto di stato e si regola tutta la rete. Ecco che la riflessione sul non-luogo di Internet trova un approdo concreto, i confini territoriali smettono di essere determinanti, la regola può essere potenzialmente applicata in tutto il mondo. A livello teorico, è stato appunto sostenuto che le norme tecniche eviterebbero così il problema dell'applicazione delle leggi statuali e dell'armonizzazione del diritto; la stessa rete risulterebbe la giurisdizione di riferimento[22].

Inoltre, l'utente del sistema informatico gioca un ruolo attivo, dato che, se previsto dalla struttura tecnologica, può personalizzare le opzioni di azione e può farlo a basso costo[23]. Si sottolinea, però, che le opzioni del sistema devono pur sempre essere conformi all'ordinamento statuale, nel rispetto della legalità. La responsabilizzazione dell'utente è un obiettivo diffuso e un tema caldo in diversi contesti. In via esemplificativa, a livello europeo, il piano d'azione dell'Agenda Digitale dell'*e-Government* per gli anni dal 2011 al 2015 contiene al primo posto la priorità della responsabilizzazione degli utenti, con lo scopo di migliorare l'efficacia e il dinamismo dell'amministrazione europea nel suo complesso[24].

[22] Si veda l'opinione di FINOCCHIARO, *Riflessioni su Diritto e Tecnica*, cit., 836.

[23] REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, cit., 572*: "The customization process shows a number of significant differences between the legal regime and Lex Informatica. Law allows customization either through high cost, individualized contract negotiations, or through the moderate-cost use of standardized forms. Lex Informatica offers a wider range of options. Off-the-shelf configurations, like those contained in software packages bundled with equipment, are a relatively low-cost customization of rules"*.

[24] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, del 15 dicembre 2010, intitolata «Il piano d'azione europeo per l'eGovernment 2011-2015 - Valorizzare le TIC per promuovere un'amministrazione digitale intelligente, sostenibile e innovativa».

A questo punto si può affermare che i sistemi informatici possono essere conformati al diritto e possono adeguarsi alle scelte dell'utente. La *lex informatica* offre una tutela *ex ante*, al contrario della tipica tutela legale che opera *ex post*. L'efficienza del diritto allora può essere maggiore. La conformazione delle tecnologie al dettato normativo permette un indubbio innalzamento del livello di prevenzione, rendendo lo strumento inadatto alla commissione di attività dannose o vietate[25].

Il diritto ha questa possibilità: può utilizzare la tecnologia come strumento, può influenzarne lo sviluppo[26]. Si è sostenuto che lo strumento tecnologico è tale da consentire di raggiungere un nuovo modo di rappresentazione del diritto, che diventa non lineare e discontinuo, consente di moltiplicare le sue possibilità di cognizione, grazie alle banche dati informatiche, anche di archiviazione e di conservazione del diritto, sempre maggiore e ottimizzato, e infine conduce a nuove forme di tutela[27]. Affinché tutto ciò sia realizzabile, la norma giuridica deve essere espressa in termini che ne permettano un trattamento automatico da parte del sistema informatico, con la conseguenza che si possono perdere delle sfumature interpretative e si dovrebbero evitare le formulazioni di principio. La norma sarebbe così incorporata in una serie di bit.

Il rischio di un diritto rigido è quello di creare uno scarto tra la regola e la realtà, dal quale potrebbe derivare una debolezza o un'impossibilità regolatrice[28]. Si dovrà perciò elaborare delle norme che conservino l'attitudine ad operare anche in situazioni mutate, pur essendo inserite nella tecnologia, con lo scopo di evitare la creazione di strumenti regolativi inscindibili dal momento storico. Una possibilità è lasciare dei criteri di fondo e ampio spazio alle scelte dell'utente ed elaborare degli standards.

Per un altro verso, se si riconosce alla tecnologia e così alla rete l'esistenza di una comunità autonoma, a cui dare importanza, possono essere ritenuti rilevanti anche quegli atti in qualche modo definibili giurisdizionali, che provengono da organizzazioni preposte all'autogoverno della rete e sono finalizzati alla risoluzione di controversie *ivi* sorte[29]. Si risolverebbero tanto più i problemi di risoluzione delle liti sorte in Internet dovuti alla sua natura sovranazionale[30].

---

[25] La finalità preventiva è evidenziata in M. DURANTE, U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET giuridica, Torino, 2012, 162.
[26] G. SPEDICATO, *Law as Code? Divertissement sulla lex informatica*, in *Ciberspazio e dir.*, 2009, fasc. 2, 236.
[27] *Ibidem,* 242.
[28] S. RODOTÀ, *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in *Riv. crit. dir. priv*, 2004, fasc. 3, 372.
[29] L'ambito della risoluzione delle controversie è inserito in DE ROSA, *La formazione di regole giuridiche per Il "Cyberspazio"*, cit., 361.
[30] MANTELERO, *Regole tecniche e giuridiche*, cit., 673.

Se i vincoli virtuali sostituissero le regole giuridiche si creerebbe un forte impatto sulla vita del diritto e sulla psicologia giuridica[31].

Ad avviso di chi scrive, non è pensabile la creazione di due sistemi di regole parallele con fonti separate nel diritto o nella tecnologia, ma è piuttosto concepibile un sistema legale integrato che sfrutti la tecnologia e il suo essere strutturata e strutturabile per rendere più efficaci le norme giuridiche comportamentali. Questa soluzione certamente comporta dei costi per il mercato e per i vari prodotti, ma verrà operato un bilanciamento dei vari interessi.

C'è chi fa notare che questa strada non può essere l'unica e la sola soluzione, perché la collaborazione tra diritto e tecnica è solo un'altra strada da percorrere oltre alla definizione di modelli comportamentali[32], con le consuete norme giuridiche poste dal legislatore; tuttavia allo stesso tempo non si esclude mai l'importanza e l'innovazione di questa metodologia.

Appare intuitivo il fatto che non si potrà conformare ogni sistema tecnico, ogni codice, ma si dovrà operare nella zona del possibile, ove la regola giuridica sia concretamente traducibile in una serie di bit, e ove invece ci si trovi di fronte ad una situazione di impossibilità soccorrerà la tradizionale prescrizione di obblighi e divieti.

Non si dimentica che un esempio concreto di implementazione di regole giuridiche nella tecnologia è già da tempo previsto in un altro ambito giuridico toccato dall'evoluzione tecnologica, ossia la proprietà intellettuale, tutelabile con le misure tecnologiche di protezione[33].

In questa tesi si cercherà di approfondire la questione in ambito di privacy, in particolare analizzando e contestualizzando il principio di privacy by design[34]. Unire le norme giuridiche e le misure tecniche per garantire la privacy conduce a delle soluzioni che sono delle *"spie da utilizzare per far crescere la consapevolezza sociale dei temi riguardanti il modo in cui l'identità deve essere considerata nel nuovo ambiente tecnologico"*[35].

---

[31] Così si profila in G. SARTOR, *Il diritto della rete globale*, in *Ciberspazio e dir.*, 2003, fasc. 1, 67-94.

[32] Così scrive A. MANTELERO*, Digital privacy: tecnologie "conformate" e regole giuridiche* in F. BERGADANO, A. MANTELERO, G. RUFFO, G. SARTOR (a cura di), *Privacy digitale. Giuristi e informatici a confronto,* Giappichelli, Torino, 2006, 38.

[33] Si vedano: G. SPEDICATO, *Le misure tecnologiche di protezione del diritto d'autore nella normativa italiana e comunitaria*, in *Ciberspazio e dir.*, 2006, fasc. 4, 535-580; R. CASO, *La Corte di giustizia e la tutela delle misure delle tecnologiche di protezione del diritto d'autore: cinquanta (e più) sfumature di grigio*, Nota a CGUE sez. IV 23 gennaio 2014 (causa C-355/12), in *Foro it*., 2014, 207-210.

[34] A. CAVOUKIAN, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian*, *IDIS* (2010) 3: 247.

[35] Sono le parole di S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Bari, 2012, 337.

2. L'importanza dell'interdisciplinarietà dell'approccio ai problemi

Ancora prima di ripercorrere le tappe fondamentali della tutela della privacy, risulta opportuno fare qualche accenno alla questione dell'interdisciplinarietà del sapere.

Oggigiorno, ancor più che in passato, per risolvere i problemi giuridici, non è più possibile porsi con l'unico punto di vista del diritto, perché le scienze e le discipline sono solo categorie che non colgono le sfumature della realtà[36].

Per quanto riguarda, ad esempio, la criminologia, l'approccio interdisciplinare è molto presente, forse perché sin dalle origini si identifica come una *"costellazione di diverse e numerose discipline, che collaborano per uno scopo ben definito"*[37]. Si pensi, poi, al rapporto tra diritto civile e scienze cognitive: l'incontro tra le due discipline conduce a nuove soluzioni per molti problemi giuridici, come l'affidabilità di una testimonianza o la valutazione di una prova durante un processo[38].

Nell'ambito del dialogo tra il diritto e la tecnologia, in particolare, è auspicabile una visione integrata di diversi tipi di professionalità: informatica, giuridica, organizzativa. Ogni problema dovrebbe essere affrontato non come di esclusiva competenza dell'informatico o del giurista, dal momento che sono necessarie sempre più competenze e più professionalità di quelle appartenenti ad una sola carriera, con l'attenzione di valorizzare sempre il dialogo, la comprensione reciproca e il rispetto dei ruoli di appartenenza[39].

Gli ingredienti del approccio interdisciplinare sono appunto[40]: l'umiltà dell'approccio, la ricerca di tassonomie comuni, l'assunzione della complessità del problema, la logica dello zoom per raggiungere allo stesso tempo il particolare e il generale, evitare alcuni pericoli, come la specializzazione estrema, la formazione a "T" (ossia, avere la radice salda nel proprio sapere e i

---

[36] G. PASCUZZI, *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica*, Bologna, Zanichelli, 2013, 185: *"Le discipline sono fenomeni culturali storicamente collocati e determinati. Esse nascono come strumento per governare l'accumulo dei saperi: l'esplosione della conoscenza ha reso necessario classificarla (un po' come avviene per la classificazione dei libri nelle biblioteche). Ma non bisogna dimenticare che se la scienza è disciplinare non lo è la natura e non lo sono i problemi da affrontare".*

[37] Un'analisi dell'approccio interdisciplinare in materia criminologica è contenuto in G. CANEPA, *Criminologia e scienze criminali. Un approccio interdisciplinare nella prospettiva medico-legale*, in *Riv. it. med. Leg.*, 1990, fasc. 2, pt. 1, 390.

[38] Si veda C. BONA, R. RUMIATI, *Psicologia cognitiva per il diritto*, Bologna, Il Mulino, 2013; da cui lo studio in alcuni corsi universitari, tra cui all'Università di Trento, del diritto civile e scienze cognitive, come branca del diritto in cui si studia l'influsso degli studi psicologici sui problemi giuridici.

[39] FINOCCHIARO, *Riflessioni,* cit., 839.

[40] Per maggior completezza e descrizione si veda PASCUZZI, *La creatività del giurista,* cit., 185-186.

rami in rete con gli altri), l'importanza dei mediani, i cosiddetti metodologi del dialogo, e il lavoro di squadra, in cui il giurista potrebbe porsi da leader.

La creazione di un ponte tra diritto ed informatica con un approccio interdisciplinare è una visione presente nel panorama dottrinale attuale. In relazione ai sistemi multi-agente, un autore riferisce che le barriere linguistiche tra i giuristi e i software engineers sono il primo ostacolo da superare, ma che questo può essere risolto con un approccio interdisciplinare, rendendo possibile l'interconnessione delle ricerche e un lavoro comune che sia svolto in una modalità reciprocamente vantaggiosa[41]. L'oggetto da affrontare con un approccio di dialogo tra i saperi è necessariamente di comune interesse o consiste in un problema di confine tra le due discipline. Il *boundary object* appare come un concetto, o una tematica, utilizzato e concepito in modo diverso tra più comunità di pratica, identificabili come gruppo di giuristi o di informatici, legati da una ricerca comune. Per far collaborare proficuamente queste comunità, l'oggetto della ricerca dovrà essere analizzato con i due punti di vista assieme e allo stesso tavolo.

Il giurista, dunque, non deve sentirsi spodestato da un altro professionista o non valorizzato per la sua competenza, anzi, può svolgere al meglio il suo compito, orgoglioso della sua predisposizione ad essere un possibile ponte tra i diversi saperi.

Negli Stati Uniti il "genuino" approccio interdisciplinare è stato intrapreso negli anni cinquanta, ponendo in dialogo il diritto e le scienze sociali, soprattutto nell'ambito della criminologia e con la creazione di nuovi corsi di sociologia del diritto[42]. Oggi, all'interno dei programmi di varie università americane è possibile notare che vi è ancora oggi la tendenza a questa metodologia di insegnamento, come accade all'università di Harvard[43] o a quella di Berkeley[44].

Anche in Italia sono presenti nuove tendenze all'interno delle università a fornire una formazione più ad ampio spettro, che consenta al giurista di apprendere delle basiche nozioni da informatico. Non a caso, alcuni corsi di

---

[41] Così in M. LAUKYTE, *An interdisciplinary approach to multi-agent systems: bridging the gap between law and computer science*, in *Informatica e dir.*, 2013, fasc. 1, 223-224: *"I do not speculate about the causes of this language barrier, but I do point out that one way in which it can be taken down is an approach that – by bringing to bear the sociological concept of a boundary object, understood as an interactive object lying at the boundary between different disciplines – makes it possible for the relative research communities to relate to one another and work together in a mutually beneficial way (here, in building a legal MAS)."*

[42] J. LADINSKY, *The teaching of law and social science courses in the United States*, in *Sociologia dir.*, 1976, fasc. 1, 53: *"It was during the 1950s that the genuine cross-disciplinary research efforts gradually began. The stimulus way, I suspect the recognized need legal scholars for collaboration if one were to do systematic and large-scale empirical social research, which had by then come to characterize post-war American social science."*

[43] Si veda il sito del corso di Harvard: <http://hls.harvard.edu/dept/academics/programs-of-study/law-science-and-technology/>.

[44] Allo stesso modo per il corso dell'Università di Berkeley: <https://www.law.berkeley.edu/php-programs/courses/coursee.php?cID=18509&termCode=B&termYear=2017>.

diritto dell'informatica offrono dei seminari con degli informatici, ma si deve ammettere che non è una scelta così diffusa.

L'approccio interdisciplinare, concludendo, è uno strumento utile per la risoluzione di problemi, vantaggioso per la formazione del giurista e, si potrebbe aggiungere, valido per la stessa salute dell'università italiana e della preparazione che dovrebbe offrire per affrontare il temuto e sognato mondo del lavoro[45].

3. La nascita e l'evoluzione della tutela della privacy

C'era una volta a Boston un giovane avvocato, il quale sposò la figlia di un ricco senatore e iniziò a vivere una vita molto mondana. Il prezzo del successo fu l'attenzione pressante e fastidiosa della cronaca giornalistica e così l'avvocato dovette chiedere aiuto ad un collega per risolvere i suoi problemi [46]. Da lì, da una faccenda semplice quanto una favola o una storiella, "nacque" la privacy.

Nel 1890 Warren e Brandeis pubblicarono l'articolo, ormai celeberrimo, intitolato *"The Right to Privacy"* sulla rivista giuridica *Harvard Law Review* e definirono un nuovo diritto, la privacy, come *the right to be let alone*[47]. Già prima, in realtà, alcuni giudici americani avevano deciso nel senso di proteggere dei cittadini dagli attacchi del giornalismo scandalistico, ma è solo con il saggio dei due giuristi che si ha una riflessione teorica sul tema e storicamente si fa risalire la nascita della privacy. I due autori, più nel dettaglio, affermarono che il principio che consente la protezione degli scritti e di ogni produzione personale degli individui, prevenendo una loro pubblicazione indebita, non è in realtà la proprietà privata, ma, invece, il principio che

[45] In merito alla salute dell'università italiana sono interessanti le parole di F. GALGANO, *Dibattito a più voci intorno alla crisi dell'università italiana e al libro di Vincenzo Zeno Zencovich, Ci vuole poco per fare una università migliore. Guardando oltre la "riforma Gelmini",* in *Contr. impr.*, 2012, fasc. 2, 315: *"L'approccio interdisciplinare nell'analisi dei problemi della società civile dovrebbe essere favorito così come nel mondo dell'imprenditoria il lavoro in équipe è già un'esperienza acquisita. Naturalmente occorre salvaguardare la specificità dei vari settori disciplinari e dobbiamo augurarci che i giuristi, che hanno il compito di formare dei professionisti, conservino un ruolo autonomo nell'istituzione. Ma dobbiamo confrontarci con gli altri. Purtroppo uno fra i tanti mali che affliggono l'Università italiana è questa incapacità di stare insieme e di lavorare a progetti di ricerca o formazione in gruppi di ricercatori, ognuno portatore di esperienze di studi diverse, in funzione del raggiungimento di obiettivi comuni".*

[46] E in particolare, quello che viene definito *yellow journalism* in Collins English Dictionary, Complete and Unabridged, HarperCollins Publishers, 12th Edition 2014: *"the type of journalism that relies on sensationalism and lurid exaggeration to attract readers" (perhaps shortened from the phrase Yellow Kid journalism, referring to the Yellow Kid, a cartoon (1895) in the New York World, a newspaper having a reputation for sensationalism)".*

[47] S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, 4 *Harv. L. Rev.* 193 (1890).

garantisce un'inviolate personality[48]. Tuttavia, Il "diritto ad essere lasciati soli" nella propria vita privata non impedisce la pubblicazione di ciò che è di pubblico o generale interesse[49]; se all'opposto l'interesse è privato, nemmeno l'assenza di mala fede esime la condanna: l'individuo ha diritto ad essere protetto tanto quanto viene protetta la sua proprietà privata.

A partire da questa importante elaborazione dottrinale la privacy è stata tutelata negli Stati Uniti con il principale scopo di fornire una protezione adeguata rispetto alle intrusioni governative non autorizzate che violino la vita privata del cittadino. Innanzitutto, la protezione è stata garantita con varie fonti del diritto, tra loro profondamente diverse, tra le quali degli istituti di common law, attraverso la tort law o la contract law, le regolazioni della statutory law, sia federale (come, ad esempio, il *Privacy Act* del 1974[50]) sia statale, frammentando e settorializzando notevolmente la disciplina, e l'apporto della costitutional law, soprattutto grazie all'apporto giurisprudenziale delle corti, che hanno interpretato estensivamente il primo e quarto emendamento della Costituzione in più di un'occasione, pur in assenza di un esplicito riferimento alla privacy[51].

Qualche anno dopo il saggio di Warren e Brandeis, concentrandosi ora sul contesto a noi più vicino, in Europa la dottrina intraprese una riflessione sulla categoria dei diritti alla personalità e in Germania, prima di tutti, fu definito il nuovo "diritto sulla propria sfera di segretezza"[52], invocando a riferimento legislativo il paragrafo 826 del Codice Civile Tedesco.

La dottrina italiana degli inizi del Novecento rifletté parimenti su questa tematica, prendendo a modello la dottrina tedesca. Un importante contributo degli anni trenta preferì parlare di *"diritto alla illesa intimità privata"*[53], perché

---

[48] *Ibidem, 205: "The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality".*

[49] *Ibidem*, 214: *"The right to privacy does not prohibit any publication of matter which is of public or general interest".*

[50] Sul sito del dipartimento di Giustizia degli Stati uniti, <https://www.justice.gov/opcl/privacy-act-1974>, a propostito del *Privacy Act* si legge: *"The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual".*

[51] U. PAGALLO, *La tutela della privacy negli Stai Uniti d'America e in Europa, modelli giuridici a confronto,* Giuffrè, Milano, 2008, 61: "*La privacy è stata così riconosciuta come oggetto di tutela in rapporto sia alla vita pubblica delle persone sia alla loro sfera privata, tenuto conto di quanto previsto soprattutto dal primo e quarto emendamento alla Costituzione. Mentre, nel primo caso, la privacy è garantita in nome dei principi di libertà d'espressione e di associazione, nel secondo caso, invece, si tratta del diritto alla sicurezza per la propria persona, abitazione, documenti ed effetti, contro ogni irragionevole intrusione dello stato e del governo"*.

[52] Lo riporta M. FERRARA SANTAMARIA, *Il diritto dell'illesa intimità privata*, in *Riv. dir. priv.*, vol. I, 1937, 169.

[53] *Ibidem,* 170.

scrivere di diritto alla riservatezza, si legge, sarebbe stato poco comprensibile. Si definì in quelle pagine un diritto assoluto e inviolabile, a tutela dell'intimità della persona indipendentemente dalla dimostrazione di un danno effettivo, e a scapito dell'indiscrezione e della curiosità altrui. Si cercò un appiglio normativo a varie norme civili e penali, come ad esempio, la disposizione sul diritto all'immagine dell'allora vigente legge sul diritto d'autore del 7 novembre 1925 n. 1950.

La riflessione sul riserbo dall'indiscrezione altrui riguardò soprattutto le persone notorie e l'abusiva pubblicità in cui spesso venivano coinvolte[54].

È proprio in ragione della tutela della vita privata di persone famose che la giurisprudenza italiana affrontò il problema della riservatezza.

La Corte di Cassazione nella sentenza del 22 dicembre 1956, n. 4487 si trovò per la prima volta a decidere sulla questione della sussistenza e dei limiti del diritto alla riservatezza e negò, con riferimento al famoso caso Caruso, la presenza di un tale diritto[55], ponendosi in contrasto con il prevalente pensiero giuridico della dottrina italiana[56], la quale invocava uno sforzo interpretativo a vantaggio della tutela della vita privata e del diritto alla personalità.

Sette anni più tardi la Cassazione ribadì l'inammissibilità del diritto alla riservatezza nella sentenza del 20 aprile 1963 n. 990[57], ma stabilì che la divulgazione di notizie relative alla vita privata, in assenza di un consenso quantomeno implicito e di un interesse pubblico alla conoscenza della vicenda, violava il diritto assoluto di personalità, ossia il diritto all'autodeterminazione dell'individuo come singolo. Si ebbe, quindi, un riconoscimento *"sostanziale, ma non verbale, del diritto alla riservatezza"*[58], perché mancava ancora un'esplicita previsione del legislatore e una costruzione giuridica interpretativa più elaborata.

Soltanto in seguito a queste due pronunce, il Supremo Collegio, con la sentenza del 27 maggio 1975 n. 2129 sul caso di Soraya Esfandiari[59], affermò

---

[54] *Ibidem,* a pag. 184, si legge, suscitando oggi una simpatia per gli esempi proposti: *"Si pensi alla notizia dell'effettiva età di una signorina o di una signora",* o la *"menzione che la persona è stata legittimata per susseguente matrimonio dei suoi genitori, mentre notoriamente è ritenuta di filiazione legittima, non già legittimata".*

[55] Cass., Sez. I civile, 22 dicembre 1956 n. 4487, in *Foro It.* 1957, vol. 80, 9: *"Nessuna disposizione di legge autorizza a ritenere che sia sancito, come principio generale, il rispetto assoluto alla intimità della vita privata e tanto meno come limite alla libertà dell'arte".*

[56] In questo senso A. DE CUPIS, Nota a sentenza, in *Foro It.* 1957, vol. 80, Parte I-16, 234: *"Le idee, dunque, della Cassazione sui diritti della personalità, sui beni che di questi costituiscono l'oggetto, sul significato e sui limiti della tutela degli stessi beni, non sono così profonde e così rigorose come sarebbe stato necessario nel momento in cui essa si accingeva ad imprimere un nuovo corso alla giurisprudenza. In conseguenza, l'inesistenza del diritto alla riservatezza non è affatto dimostrata in questa sentenza: e lo stesso diritto, seppure non esiste per la Cassazione, continua ad essere nell'ordinamento giuridico".*

[57] Cass., Sez. I civile, 20 aprile 1963 n. 990, in *Foro It.* 1963, vol. 86, 877-879.

[58] Lo afferma A. DE CUPIS, Nota a sentenza, in *Foro It.* 1963, vol. 86, 1298.

[59] Cass., Sez. I civile, 27 maggio 1975 n. 2129, in *Foro It*. 1976, vol. 99, 2895-2907.

che il diritto alla riservatezza è riconosciuto e tutelato dall'ordinamento giuridico, in armonia con i principi costituzionali e le convenzioni internazionali. Il diritto alla riservatezza, a parere della Corte in quel leading case, consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari, nelle quali non essendoci per i terzi un interesse socialmente apprezzabile alla loro conoscenza, si ha la protezione contro le ingerenze non giustificate da interessi pubblici preminenti, sebbene siano compiute con mezzi leciti, con fini non speculativi e senza offesa per l'onore dell'individuo coinvolto.

Dalla vicenda di Warren al caso della principessa Soraya, pur coinvolgendo ordinamenti diversi, il diritto alla riservatezza corrisponde al "diritto ad essere lasciati soli" nella propria vita privata, alla protezione del soggetto nelle mura del proprio domicilio.

Nella società dominata dall'informatica si assiste ad un'evoluzione della tutela e del concetto della riservatezza; essa difatti non riguarda più solo l'individuo che vuole essere lasciato solo, ma la protezione dei dati personali e della loro circolazione dovuta allo sviluppo dei calcolatori elettronici. Il problema, si può dire, interessa gli stessi programmi elettronici[60]. La privacy assume una valenza molteplice e si riempie di nuove sfaccettature. L'ammontare gigantesco delle informazioni circolanti, la costante raccolta e la loro elaborazione hanno condotto a parlare di "società della sorveglianza" e hanno spinto a riflettere su quali fossero i connotati di una normativa in grado di rispondere ai problemi reali e ad adattarsi al cambiamento tecnologico, visto che il ritardo legislativo italiano, rispetto agli altri paesi europei, ha reso per anni il nostro stivale una sorta di "paradiso dei dati"[61].

Ad un'evoluzione di contenuto si affianca in Europa un cambiamento nella fonte del diritto attraverso la quale è possibile ottenere tutela, dal momento che a partire dagli anni settanta furono emanati i primi interventi normativi negli stati e che l'allora Comunità Europea iniziò ad interessarsi di privacy, con risvolti propulsori per il nostro Paese e più in generale per la regolazione nel vecchio continente, ruolo che oggi conserva ancora regime in qualità di Unione. Per una disciplina legislativa italiana in materia, si è dovuto attendere fino agli anni novanta del secolo scorso, durante i quali il diritto al controllo del flusso delle informazioni e dei dati (quello che si intende definire privacy 2.0) è stato garantito grazie alla spinta europea degli accordi di Schengen e all'attuazione di

[60] È di questa opinione V. FROSINI, *Informatica diritto e società*, Giuffré Editore, seconda edizione, 1992, Milano, 183: *"Nella società informatica il problema della riservatezza riguarda però gli stessi programmi elettronici: i quali possono avere per contenuto dati d'interesse personale, ma anche d'interesse "privato" perché si riferisce ad una iniziativa, ad una invenzione, ad una impresa, che possono essere definite private senza essere esattamente personali; o un contenuto, che può essere di interesse pubblico, e che va difeso dal pericolo di venire a conoscenza dei privati, come i segreti di carattere militare".*

[61] Si legge all'interno di A. BELLAVISTA, *Società della sorveglianza e protezione dei dati personali*, in *Contr. impr.*, 1996, 63-81, soprattutto per l'ambito di tutela della riservatezza nei luoghi di lavoro.

direttive comunitarie e, in particolare, alla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati". A partire da questa normativa e dall'esigenza molto sentita di un intervento legislativo[62] è stata emanata la legge 31 dicembre 1996 n. 675, per la "tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Il testo italiano non coincide esattamente con quello della direttiva, la quale ha lo scopo di conciliare la rimozione degli ostacoli alla circolazione dei dati personali tra gli stati membri a vantaggio del mercato interno e della protezione dei diritti fondamentali delle persone[63], e pone all'interprete l'interrogativo se fosse una legge che disciplinasse il trattamento dei dati personali, ovvero fosse posta a tutela della personalità, intesa negli aspetti di riservatezza e identità personale[64]. La risposta che si può dare è che la tutela del dato è una specificazione o quantomeno un'accezione diversa da quella della riservatezza e che entrambe possono convivere nella moderna privacy.

In seguito a varie modifiche della legge del '96, e alla direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al "trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche" è stato elaborato dal nostro legislatore il Decreto Legislativo del 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali (d'ora in avanti: Codice Privacy), pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 (Supplemento Ordinario n. 123). All'articolo 2 sulle finalità del codice si specifica che la tutela è prevista con riferimento alla riservatezza, all'identità personale degli individui e al diritto alla protezione dei dati personali. La riservatezza e la protezione dei dati personali convivono esplicitamente nel nuovo sistema di regole. La definizione di dato personale che viene inserita nel decreto è: "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"[65]. Si è in presenza di una reificazione del dato personale, che è oggetto di disciplina giuridica per il solo fatto di essere connesso ad un soggetto identificabile[66]. Inoltre, con il Codice Privacy si supera la centralità assoluta

[62] Lo stesso autore del contributo del 1937 ritorna sul tema con M. FERRARA SANTAMARIA, *Il diritto alla illesa intimità privata "right of privacy"*, in *Dir. aut.*, 1996, fasc. 4, 403: *"È un problema di grande attualità e va affrontato legislativamente senza indugi".*

[63] Si veda F. BALDUCCI ROMANO, *La Protezione dei dati personali nell'unione Europea tra libertà di circolazione e diritti fondamentali dell'uomo,* in *Riv. It. dir. pubbl. com.*, 2015, fasc.6, 1623.

[64] L'interrogativo è specificato in V. Z. ZENCOVICH, *Una lettura comparatistica della L. n. 675/96 sul trattamento dei dati personali,* in *Riv. trim. dir. proc. civ.*, fasc.3, 1998, 734.

[65] Cfr. Art 4, comma 1, lett. b). D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

[66] Sulla reificazione V. Z. ZENCOVICH, *I diritti della personalità*, in N. LIPARI, P. RESCIGNO (a cura di), *Diritto civile*, vol. 1, Giuffré, 2009, 553.

della volontà del singolo nel prestare o meno il consenso sui propri dati e si interviene sulle modalità del trattamento, in modo da assicurare una tutela minima[67] ad ogni dato circolante.

Considerando più in generale tutto il sistema delle fonti, ad oggi la privacy è protetta chiaramente a livello costituzionale in modo implicito grazie alla tutela del valore assoluto della persona umana di cui agli articoli 2 e 3 della nostra Carta Fondamentale[68]. Non solo, il diritto alla protezione dei dati personali è stato acquisito tra i diritti fondamentali dell'Unione Europea[69] grazie alla presenza nella Carta dei diritti fondamentali dell'Unione dell'articolo 8, che stabilisce che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano e che tali dati devono essere trattati secondo il principio di lealtà, utilizzati per finalità determinate e raccolti in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge. Ogni individuo, in più, ha il diritto di accedere ai dati raccolti e di ottenerne la rettifica, qualora siano mutati e variate le circostanze[70]. Attraverso l'articolo 6 del Trattato di Lisbona[71], che rende la Carta di Nizza del 7 dicembre 2000 vincolante ai sensi dei Trattati Europei, e la giurisprudenza favorevole della Corte di Giustizia, il diritto in esame figura così tra i diritti fondamentali dell'Unione Europea[72]. La Corte di Giustizia, alla cui posizione si vuole soltanto

---

[67] Sull'intervento del Codice si veda A. MANTELERO, *Privacy*, in *Contr. impr.*, 2008, fasc. 3, 779.

[68] È di questo avviso D. GRANARA, *Il fronte avanzato del diritto alla riservatezza,* in *Riv. it. dir. pubbl. com*, 2015, fasc.3-4, 902.

[69] In questo senso è stato fondamentale l'apporto del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, che nella Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali adottata, adottata il 7 settembre 1999 si esprimeva così: *"Includere la protezione dei dati personali nel quadro dei diritti fondamentali europei significherebbe rendere tale protezione giuridicamente vincolante in tutta l'Unione e tener conto della crescente importanza della protezione dei dati nella società dell'informazione. Il Gruppo raccomanda pertanto alla Commissione europea, al Parlamento europeo e al Consiglio dell'Unione europea di includere il diritto fondamentale alla protezione dei dati personali nella Carta dei diritti fondamentali. Il Gruppo è disposto a collaborare all'elaborazione della Carta".*

[70] Cfr. Art. 8, Carta dei Diritti Fondamentali dell'Unione Europea del 7 dicembre 2000.

[71] Cfr. Art. 6, co.1, 1 Trattato sull'Unione Europea: "*L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni*".

[72] BALDUCCI ROMANO, *La Protezione dei dati personali,* cit., 1657: *"Ancor più rilevante appare la definitiva acquisizione del diritto alla protezione dei dati personali tra i diritti fondamentali dell'Unione. Attraverso il nuovo testo dell'art. 6 del TUE, il diritto in esame figura oggi a buon titolo tra i diritti fondamentali dell'Unione. Esso è autonomo non tanto perché esiste una norma ad hoc nella Carta, quanto piuttosto per il suo contenuto sostanziale: il diritto alla protezione dei dati personali si riferisce ad un bene giuridico diverso dalla riservatezza, ossia l'identità personale; esso non consiste nel mantenere il segreto, e neppure nel right to be let alone, bensì*

fare accenno, nei vari casi di cui si è occupata in materia di privacy ha affermato con decisione la sua competenza e l'importanza del modello europeo, concentrandosi sul diritto alla protezione dei dati personali su internet, dimostrando che ciò che si vuole proteggere non è tanto la vita privata, quanto le informazioni diffuse grazie alla rete[73]. La natura di diritto fondamentale è strenuamente difesa e messa in bilanciamento con gli altri interessi via via coinvolti nelle fattispecie giudiziali.

Per di più, l'articolo 16 del Trattato sul Funzionamento dell'Unione[74] ha conferito la base giuridica per l'adozione di norme di diritto derivato in materia di protezione dei dati personali, ampliando così la competenza dell'Unione[75]. Proprio dal riferimento alla suddetta base normativa è iniziato il processo di elaborazione di un regolamento europeo in materia di protezione dei dati personali, di cui verrà dato conto nel prossimo paragrafo.

Primariamente, riflettendo sul corso evolutivo di questo diritto, si può affermare, dunque, che con l'evoluzione informatica si ha il passaggio da un diritto negativo, volto ad escludere l'altro, l'ingerente, con il fine di essere lasciati in pace nella propria intimità, ad un diritto positivo, che consente di disporre del controllo dei propri dati e di conseguenza della propria libertà. La "libertà informatica" è garantita affinché l'individuo possa controllare la circolazione dei suoi dati[76]. Spesso non è più sufficiente neppure questo, perché la tutela della riservatezza oggi non si riferisce più soltanto alla persona come tale, e nemmeno ai suoi dati, ma ancor più al procedimento di

---

nel potere di controllare i propri dati personali, a prescindere dal fatto che essi siano privati o pubblici".

[73] Si esprime in questo senso G. FINOCCHIARO, *La Giurisprudenza della Corte di Giustizia in materia di dati Personali da Google Spain a Schrems*, in *Dir. informazione e informatica*, 2015, fasc.4-5, 797.

[74] Cfr. Art. 16 del TFUE (ex articolo 286 del TCE): "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. 3. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea*".

[75] Una riflessione in merito è di G. F. AIELLO, *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale "disomogeneo" alla luce della nuova proposta di "General Data Protection Regulation"*, in *Oss. dir. civ. comm*., 2015, fasc. 2, 427*: "L'approvazione dell'art. 16, viceversa, incide sulle prerogative di un ente a competenza non generale come l'UE fornendo a quest'ultima, per la prima volta, «una base giuridica specifica» per l'adozione di norme sul trattamento dei dati personali. L'approvazione delle direttive emanate a partire dal 1995, in mancanza di una norma del genere, era stata giustificata sulla base delle competenze in materia di instaurazione e rafforzamento del mercato interno. L'armonizzazione della disciplina, pertanto, era unicamente finalizzata alla tutela della concorrenza mediante la rimozione degli ostacoli all'esercizio di attività economiche su scala comunitaria".*

[76] Si definisce la libertà informatica in FROSINI, *Informatica diritto e società*, cit., 244.

elaborazione degli stessi, *"alla loro teleologia, ossia all'obiettivo a cui è mirato il procedimento"*[77]. La libertà positiva di esercitare un controllo sul flusso delle proprie informazioni fa sì che il diritto alla protezione dei dati personali venga inteso come il diritto all'autodeterminazione informativa, ossia il diritto alla possibilità di ogni individuo di autodefinirsi e determinarsi[78]. Si tutela il modo di essere e di vivere dell'individuo, la sua libertà personale ed esistenziale e in tal modo si garantisce che la società sia parimenti libera[79].

4. La General Data Protection Regulation

L'ultima novità all'interno del quadro normativo europeo, che segna un passo decisivo per l'evoluzione della privacy, è la General Data Protection Regulation*,* il Regolamento Generale sulla Protezione dei Dati dell'aprile 2016*.*

Necessaria premessa a questa normativa è la pubblicazione nel 2010 del Programma di Stoccolma, ossia del piano quinquennale dell'Unione Europea in materia di sicurezza e giustizia per il periodo 2010-2014[80]. Il Consiglio Europeo, ricordando che il diritto al rispetto della vita privata e alla protezione dei dati personali è sancito dalla Carta dei diritti fondamentali, statuisce che l'Unione deve garantire una strategia globale in materia di protezione dei dati, promuovendo l'applicazione dei vari principi e assicurando il massimo rispetto della vita privata. Il Consiglio esprime la convinzione che i progressi tecnologici, malgrado pongano nuove sfide in termini di protezione dei dati personali, offrono allo stesso tempo delle nuove possibilità per garantire una migliore protezione. In più, il Consiglio invita la Commissione a valutare il funzionamento dei vari strumenti europei per la protezione dei dati e a presentare, se necessario, iniziative complementari, legislative o meno[81]. Si chiede così di proporre un quadro giuridico completo in materia di protezione dei dati, revisionando la direttiva 95/46/CE.

Nel piano d'azione per l'attuazione del programma di Stoccolma il 25 gennaio del 2012 la Commissione Europea pubblica la proposta di regolamento sulla protezione degli individui con riguardo al trattamento dei dati personali e

---

[77] *Ibidem*, 309.
[78] FINOCCHIARO, *La Giurisprudenza cit.*, 784.
[79] A tal proposito si riportano le parole dell'intervista al già presidente del Garante per la Protezione dei Dati Personali, in S. RODOTÀ, *Intervista su privacy e libertà*, (a cura di) P. CONTI, Laterza, Bari, 2005, 18: *"L'ultimo passaggio, legato alle nuove tecnologie e al problema della sicurezza, vede un concetto di privacy sempre più strettamente legato alla tutela della libertà personale, esistenziale: il diritto di poter compiere le mie scelte, di mantenere le mie caratteristiche non solo senza subire alcun tipo di discriminazione, ma anche senza perdere interi pezzi di identità nei mille meccanismi delle nuove tecnologie".*
[80] Consiglio Europeo, Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini, 2010/C 115/01.
[81] Programma di Stoccolma, 10-11.

sulla circolazione dei dati, che sostituisse la direttiva 95/46/CE[82]. La Commissione espone primariamente il contesto della proposta e spiega che il rapido sviluppo tecnologico ha portato a nuove sfide per la protezione dei dati personali, vista la condivisione e la raccolta di dati a larga scala da parte sia di soggetti privati sia di autorità pubbliche; la tecnologia, si legge ancora, ha trasformato l'economia e la vita sociale[83]. La Commissione pertanto ritiene che sia arrivato il momento di instaurare un quadro giuridico europeo più solido e coerente, in modo da consentire lo sviluppo dell'economia digitale nel mercato interno, garantire alle persone fisiche il controllo dei loro dati personali e rafforzare la certezza giuridica e operativa per i soggetti economici e le autorità pubbliche[84]. Su questa proposta si ritornerà quando si affronterà, nel secondo capitolo di questa tesi, il principio di protezione dei dati personali sin dalla progettazione, ovverosia la meglio definita privacy by design, perché vista la presenza dell'articolo 23, si afferma che le misure tecniche fanno oggi parte della protezione dei dati personali.

In commento alla proposta del 2012 si osserva che, nei fatti, la maggior parte dei principi contenuti nella Direttiva 95/46/CE verranno conservati nel nuovo regolamento, il quale si pone come una modernizzazione della vecchia regolamentazione e un ampliamento della protezione degli individui[85]. Si denota poi la presenza del necessario bilanciamento tra i forti interessi economici dei giganti di Internet e la libertà degli individui, i consumatori dei vari servizi offerti in rete, forzati spesso a prestare il proprio consenso in situazioni di non adeguata trasparenza. La proposta nella ricerca del giusto equilibrio tra i due interessi privilegia un approccio di tipo contrattuale tra il fornitore del servizio e

[82] Si è letta nella sua versione inglese: *Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012*.

[83] Nella Proposta, nella versione inglese, 1: *"Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life".*

[84] *Ibidem,* 2.

[85] A tal proposito A. JAMMET, *The evolution of EU law on the protection of personal data,* 3 *European (Legal) Studies on-line papers, Queen's University Belfast - School of Law* 1 (2014), 11: *"In fact, most of these principles will be conserved inside the new Regulation, which will even try to strengthen these principles71. It is presented as a modernisation of the old Directive. It includes the possible use of online identifiers or genetic identification techniques inside the data subject definition, as well as the definition of biometric and genetic data (Article 4). However, the real interest re-sides inside the enlargement of the data subject protection. Firstly, concerning the treatments, we can observe that the overall emphasis is put on the transparency and clarification of information given to the data subject".*

l'utente fruitore[86]. Tutto ciò fa emergere una concezione della privacy che potrebbe essere associata ad una parte della dottrina americana, la quale abbraccia la logica proprietaria dei dati personali[87]. In aggiunta, si è ritenuto che le nuove regole della proposta rappresentassero un vantaggio per le società europee nella competizione globale, permettendo loro di assicurare ai clienti che i dati fossero trattati con la necessaria cura e diligenza e un incentivo per gli investitori, vista la certezza del diritto offerta da un sistema generale di regole[88].

Nel marzo del 2014 il Parlamento Europeo vota in sessione plenaria per supportare in prima lettura la proposta della Commissione, già variamente emendata[89], e approva il testo con una larga maggioranza[90]. La versione votata dal Parlamento è diversa da quella della Commissione, perché introduce, ad esempio nuovi principi a cui il trattamento dei dati deve essere conforme, tra i quali l'accountability (il titolare del trattamento deve dimostrare che il suo operato è svolto in conformità del regolamento) e questa differenza tra i due testi è importante, dal momento che dimostra che la versione del 2014 tiene maggior conto di come la raccolta e l'utilizzo dei dati sono evoluti con le nuove tecnologie[91].

A questo punto è chiaro che il Regolamento creerà un quadro uniforme per la tutela dei dati. I commentatori della proposta sottolineano con forza il fatto che il futuro della protezione dei dati sarà affidato non più ad una direttiva, ma ad una regolamentazione di più alto livello[92], che entrerà direttamente a far parte delle varie leggi nazionali degli stati membri in qualità di norma

---

[86] *Ibidem*, 18: *"In the search for an equilibrium between the economic and public interests, its analysis shows that this reform is leaning to-ward a contractualisation movement of the relationship between the user and the service".*

[87] Si veda ad esempio l'autorevole P. M. SCHWARTZ, *Property, Privacy, and Personal Data*, 117 *Harv. L. Rev.* 2055 (2004).

[88] V. REDING, *The European data protection framework for the twenty-first century,* 2 *IDPL* 119 (2012), 129: *"The new rules also give EU companies an advantage in global competition. Under the reformed regulatory framework, they will be able to assure their customers that valuable personal data will be treated with the necessary care and diligence. Trust in a coherent EU regulatory regime will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services".*

[89] Il testo è pressoché aderente a quello proposto dal Comitato designato dal Parlamento Europeo con il Report finale con circa 196 emendamenti (LIBE Committee Report).

[90] Si contano 621 voti a favore, 10 contrari e 22 astenuti.

[91] Si legga F. GILBERT, *Proposed EU data protection regulation - issues to consider when planning for the future regime,* 17 *JIL* 1 (2014), 3: *"The divergence between the EU Commission Version and the EU Parliament Version is important. The EU Commission Version merely restates principles that have been in effect for almost 20 years. The EU Parliament Version, on the other hand, is more refined. It takes into account how data collection and data use has evolved with the adoption of new technologies, and brings a more contemporary approach".*

[92] Il regolamento ha portata generale ed è vincolante per gli Stati Membri ai sensi del secondo comma dell'articolo 288 del Trattato sul Funzionamento dell'Unione Europea: "*Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri*".

sovranazionale[93]. Ciò dimostra, a parere dello stesso autore citato, che il trattamento dei dati non può più essere confinato dai limiti fisici dei vari stati, ma che è piuttosto necessaria una posizione globale dell'Unione in merito, anche se dovesse suscitare delle perplessità per la "diminuzione" della sovranità nazionale. In aggiunta *ivi* si legge che la sfida del bilanciamento tra gli interessi economici e la protezione degli individui è ardua per il regolamento; la speranza è che possa contribuire a rendere solida la protezione, ma *"this is only a hope and a true tomorrow is still a long time"* e "*the best advice is to be cautious and not nurture too many expectations reconognizing that the future of data protection law is still blowing in the wind"*[94].

Un evidente passo in avanti è l'introduzione, tra i dati definiti sensibili, di tre nuove categorie legate alla salute: il dato genetico, il dato biometrico e il dato relativo alla salute[95]. Tale previsione fa apparire la proposta agli occhi di qualcuno con una sfumatura "medica", tendente al settore della salute, ossia con le caratteristiche di una legislazione specializzata[96]. Certo è che il nuovo testo rinforza la posizione degli individui, dal momento che tra le varie novità aggiunge al titolare del trattamento l'obbligo di trasparenza, prevede il diritto alla portabilità del dato[97] e il super discusso diritto all'oblio[98], rivelandosi in tal modo il prodotto migliore di anni ed anni di negoziazioni per giungere alla protezione dei dati 2.0 e riconoscere compiutamente l'importanza della tutela di uno dei diritti fondamentali dell'Unione Europea. Per quanto riguarda il trasferimento transfrontaliero dei dati "europei" il testo ne vieta l'operazione verso paesi che non offrono una protezione adeguata o conforme al regolamento; è consentito invece il trasferimento se la Commissione ha certificato che nel contesto ricettivo la protezione è adeguata o se sono presenti adeguate garanzie, in

---

[93] Sull'armonizzazione del regolamento si veda P. BLUME PETER, *It is time for tomorrow: EU data protection reform and the Internet*, 18 JIL 3 (2015).

[94] Per entrambe le citazioni molto evocative, *Ibidem*, 12.

[95] Oggi definiti dal Regolamento 2016/679 Cfr. Art. 4, comma 1, n. 13), 14), 15): "*13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; 14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; 15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*".

[96] È di questo avviso P. DE HERT, V. PAPAKONSTANTINOU, *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals,* 28 *CLSR* 130 (2012), 133.

[97] *Ibidem*, 137: *"it grants individuals the right to obtain a copy of their profiles uploaded onto internet platforms in a suitable format for further processing and use by themselves, and for such profile not to contain technical or other impediments to it being subsequently uploaded onto the internet platform of another service provider".* A tal propositivo si veda anche L. COSTA, Y. POULLET, *Privacy and the Regulation of 2012*, 28 *CLSR* 254 (2012), 257.

[98] *Ibidem*, 136-137 e in COSTA, POULLET, *Privacy and the Regulation,* cit., 256.

particolare delle “clausole tipo” di protezione dei dati, delle norme vincolanti d’impresa per il titolare del trattamento e delle clausole contrattuali[99].

La proposta non si esimia tuttavia da critiche, poiché la riforma prospetta come strumenti a disposizione delle autorità garanti solo delle sanzioni amministrative e pressoché nessuna sanzione penale[100]. Nel fare ciò si sceglie di non armonizzare il settore degli illeciti trattamenti di dati personali, che è molto frastagliato in ambito europeo, a svantaggio della certezza del diritto[101]. Ad opinione di chi scrive, però, si tratta di una scelta coerente con la natura nazionale della sovranità in materia penale.

Soltanto l’8 aprile 2016 il Consiglio Europeo ha adottato il testo e il 14 aprile si ha l’approvazione finale del Parlamento Europeo: finalmente si ottiene il Regolamento 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei Dati, d’ora in avanti GDPR) e che è stato pubblicato nella G.U.U.E. 4 maggio 2016, n. L 119[102]. Si specifica in questa sede che il GDPR è parte di un pacchetto di norme che contiene anche la direttiva 2016/680 del Parlamento Europeo e del Consiglio per regolare la protezione dei dati personali da parte delle autorità competenti a fini di prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, che sostituisce la Decisione del Consiglio 2008/977[103].

Il Regolamento Generale sulla Protezione dei Dati è entrato in vigore il 24 maggio 2016[104], ma l’effettiva applicazione è a decorrere dal 25 maggio 2018.

Il nostro Codice della privacy non verrà abrogato dal GDPR, ma essendo questo direttamente applicato, vista la sua natura normativa, è chiaro che sarà necessaria un’attività ermeneutica per poter definire quali parti saranno

---

[99] Per approfondire la questione del trasferimento transfrontaliero si veda M. ROTENBERG, D. JACOBS, *Updating The law of information privacy: the new framework of the European Union*, 36 *Harvard JLPP* 606 (2013), 636.

[100] P. DE HERT *The EU data protection reform and the (forgotten) use of criminal sanctions*, 4 *IDPL* 262 (2014), 265.

[101] *Ibidem*, 267: *“The investment of the European Union in a harmonised system of administrative sanctions and its reluctance to harmonise criminal sanctions is striking and, in my view, not defensible. The US companies in particular are intimidated by the use of criminal law, independent of its actual enforcement and the sheer existence of these provisions in some EU member states might influence their decisions and continue a process of fragmentation that the regulation was intended to halt. In view of the extensive focus on administrative wrongs, the question remains why the EU reform package has not gone all the way and harmonised the use by member states of criminal sanctions in data protection law”.*

[102] Si veda il comunicato stampa del Garante per la Protezione dei dati Personali: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718>.

[103] Per le varie informazioni sull’attuazione da parte degli organi dell’Unione Europea è utile il sito di riferimento: <http://ec.europa.eu/justice/data-protection/reform/index_en.htm>.

[104] Si veda il comunicato stampa del Garante per la Protezione dei Dati Personali: <http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5035744>.

sostituite dal testo europeo, e così implicitamente abrogate, e quali invece rimarranno ancora vigenti.

5. Ridefinire il concetto di privacy e di dato personale

Il diritto alla privacy è evoluto di pari passo con lo sviluppo tecnologico e la sua disciplina ha tentato di rimanere sempre al passo. Dare una sua definizione oggi, con un'univoca espressione, che consideri i più disparati scenari applicativi e i vari contesti in cui c'è necessità di tutela, è molto difficile. Ad opinione di molti sembra che sul concetto regni il caos[105]. La privacy può riguardare: la raccolta e la gestione dei dati personali, la protezione del corpo umano dalle procedure invasive, come le ispezioni corporali, la sicurezza delle comunicazioni interpersonali elettroniche e i limiti alle intrusioni nell'ambiente domestico, sul luogo di lavoro o negli spazi pubblici[106].

La dinamicità e l'eterogeneità del concetto sono le caratteristiche della privacy 2.0[107].

La ricerca di una soluzione per proteggere la privacy nell'era digitale è molto sentita dalla dottrina americana, la quale riflette innanzitutto sul concetto stesso del termine, spesso con un approccio molto concreto, e poi approfondisce i problemi della tipologia e della natura della fonte da cui trarre la regola applicativa, che siano codici di condotta, leggi statali o federali e persino regolamentazioni pensate su modello del nostro quadro normativo europeo[108].

Secondo l'opinione del professor Daniel J. Solove[109], la privacy può essere analizzata attraverso sei accezioni diverse: *"the right to be let alone, limited access to the self, secrecy, control of personal information, personhood, and intimacy*"[110]. L'autore analizza ciascun aspetto per dimostrare che nessuno di questi profili può essere trascurato, a meno che non si voglia restringere eccessivamente la concezione di privacy o essere troppo vaghi nel definirla. A titolo di esempio, circoscrivere la privacy come diritto al controllo dei propri dati, è un'operazione troppo restrittiva perché focalizza l'attenzione sulla scelta dell'individuo e non considera la società o il flusso più generale delle

[105] Si vedano le citazioni di espressioni di vari giuristi sulla questione in D. J. SOLOVE, *Understanding Privacy,* Harvard University Press, Boston, 2008, 1-2.
[106] B. DENTE, N. LUGARESI, M. S. RIGHETTINI (a cura di), *La politica della privacy tra tutela dei diritti e garanzia dei sistemi*, Passigli, Firenze, 2009, 267.
[107] A tal proposito è interessante la riflessione in J. E. COHEN., *What privacy is for*, 126 *Harv. L. Rev*. 1904 (2013).
[108] Per un'analisi sul tema si veda il contributo molto chiaro di W. T. DEVRIES, *Protecting privacy in the Digital Age*, 18 *Berkeley Tech. L.J.* 283 (2003).
[109] Professor of Law at the George Washington University Law School.
[110] D. J. SOLOVE, *Conceptualizing Privacy*, 90 *Cal. L. Rev.* 1087 (2002), 1094.

informazioni[111]. Solove allora propone un nuovo approccio per concettualizzare la privacy*:* l'approccio pragmatico. Come il cartografo traccia i confini delle nazioni utilizzando l'esperienza di chi ha viaggiato per scoprirle, così per il giurista è più utile mappare il terreno della privacy esaminando delle specifiche situazioni problematiche, piuttosto che cercando di ridurle tutte in una rigida categoria predefinita[112]. La privacy, in concreto, è un insieme eterogeneo di pratiche sociali, che vengono poste in essere dagli individui, e il suo valore, la necessità di tutela, dipende dallo scopo delle suddette pratiche che la coinvolgono, mutando con riferimento ad ogni particolarità. L'approccio legato alle problematiche è una visione innovativa che porta con sé delle conseguenze positive per la riflessione giuridica[113].

Lo stesso autore in un altro contributo[114], dopo aver ribadito l'importanza dell'approccio empirico, presenta una nuova tassonomia della privacy dividendo il concetto in quattro tipologie e creando così un sistema che faciliti l'analisi dei problemi, permettendo di attribuire ad ogni categoria le proprie norme giuridiche. In primo luogo, *l'information collection,* la raccolta delle informazioni, contiene al suo interno la sorveglianza e l'interrogatorio e secondariamente *l'information processing,* inteso come trattamento dei dati, comprende *l'aggregation, l'identification, l'insecurity, il secondary use* e *l'exclusion*. La terza categoria è *l'information dissemination*, la diffusione delle informazioni, la quale incorpora il *breach of confidentiality*, la *disclosure,* l'*exposure, l'increased accessibility,* la *blackmail*, *l'appropriation* e la *distortion*. All'ultimo si ha l'*invasion,* intesa come invasione, al cui interno vi è l'*intrusion* e la *decisional interference*. Questa proposta dottrinale è un esempio di riflessione costruttiva molto interessante perché evita di fornire un unico concetto del diritto alla *privacy* ed evidenzia le sue plurime accezioni.

Si palesa così un'inevitabile flessibilità del diritto alla privacy, la quale è, si potrebbe aggiungere, una vera e propria sfida per il diritto. Il nostro presente, contraddistinto dal privacy panic e da una generale sensibilità della società sul tema*,* offre la possibilità di pensare in modo creativo, fuori dagli schemi. Non si può più definire con rigidità, senza tener conto della storia della privacy e del

---

[111] *Ibidem*, 1115: *"Finally, conceptions of information control are too narrow because they reduce privacy to informational concerns, omit decisional freedom from the realm of privacy, and focus too exclusively on individual choice".*

[112] *Ibidem*, 1127: "*We should act as cartographers, mapping out the terrain of privacy by examining specific problematic situations rather than trying to fit each situation into a rigid predefmed category".*

[113] Si legga SOLOVE, *Understanding Privacy,* cit., 9: *"Therefore, my approach to conceptualizing privacy understands it pluralistically rather than as having a unitary common denominator. In focusing on privacy problems, my approach seeks to be contextual without being overly tied to specific contexts, flexible enough to accommodate changing attitudes toward privacy, yet firm enough to remain stable and useful"*.

[114] Per la tassonomia completa e la riflessione analitica si legga D. J. SOLOVE, *A Taxonomy of Privacy,* 154 *U. Pa. L. Rev.* 477 (2006).

fatto che il diritto è parte di un sistema di protezione che implica la tecnologia, le norme sociali e le pratiche dei media[115].

Lawrence Lessing nel suo *Code* riflette sui cambiamenti dovuti alla tecnologia e riporta principalmente due aspetti della privacy che variano all'interno del cyberspazio. In primo luogo, la tutela l'intimità della vita privata non può più essere legata alle barriere fisiche del domicilio dell'individuo, perché le tecnologie digitali hanno cambiato profondamente il concetto di fisicità[116]. Secondariamente, la privacy negli spazi pubblici, la quale non è generalmente garantita, ma con l'avvento della sorveglianza digitale, è aumentata esponenzialmente l'attività di sorveglianza e controllo dei cittadini in pubblico[117]. Le risposte che Lessing propone sono di quattro tipologie: il diritto, le prassi, il mercato e il codice. Così come si è detto per il diritto in generale, quindi, anche per la protezione della privacy può essere utilizzata la tecnologia.

Ciò che si vorrebbe dimostrare è che l'architettura del codice può essere creata in relazione alla privacy che si intende tutelare. Il principio di fondo che esprime questo pensiero è stato definito "privacy by design", il quale è stato scelto come tema centrale di questa tesi. Il diritto e la tecnologia, ancora una volta, smettono di essere alternativi[118]. Ridefinire la privacy alla luce di questa metodologia, comporta che essa non sia più solo un diritto spettante ad un soggetto leso nella sua sfera personale, tutelabile *ex post,* ma che abbia in sé anche la pretesa di essere tutelato *ex ante,* fin dalla progettazione, con misure tecniche e organizzative adeguate. Della protezione dei dati personali fin dalla progettazione si scriverà diffusamente nel secondo capitolo.

Non è possibile passare alla presentazione della privacy by design senza aver prima riflettuto sul rapporto tra privacy e sicurezza e sulla nozione di dato personale.

---

[115] Di questo avviso per salvare la *privacy* moderna è S. BARBAS, *Saving Privacy from History*, 61 *DePaul L. Rev.* 973, 1048: "*Like all values worth protecting, privacy cannot be defined in rigid, binary terms, reduced to simple formulae, or frozen in time. The protection of privacy should be envisioned in holistic terms; the law is part of a system for the protection of privacy that implicates technology, social norms, and media practices, and it may have a heightened role to play when other protections fail. While the exigencies of the present moment demand innovation in the law, there is also much to be had from the insights of the generation that first identified the need for a right to be let alone".*

[116] L. LESSIG, *Code*, *version 2.0*, *cit.,* 201: *"(Privacy in private) From the perspective of the law, it is the set of legal restrictions on the power of others to invade a protected space. Those legal restrictions were complemented by physical barriers. Digital technologies have changed these protections".*

[117] *Ibidem,* 223: *"The first is the threat from "digital surveillance" - the growing capacity of the government (among others) to "spy" on your activities in public".*

[118] P. GUARDA, *Data Protection, Information Privacy, and Security Measures: an essay on the European and the italian legal frameworks*, in *Ciberspazio e dir.*, 2008, 68: *"There are two levels of intervention to solve the problem: privacy law and incorporation of privacy values and principles in the digital architectures. We must avoid the false belief that they are alternative means. Some years ago we have thought that law could represent an adequate way of approaching to the problem. Now it is obvious that the digital markets are looking for a delicate balance between law and digital technology".*

Fino ad ora si è parlato di dato personale senza mai approfondire ciò che realmente significhi, ma è fondamentale procedere in questo senso perché la protezione del dato è lo scopo principale della regolamentazione della privacy. Il dato, a volte considerato un vero e proprio bene secondo certe letture proprietarie[119], circola come fosse la controprestazione della fornitura di un servizio in rete apparentemente gratuito, come una moneta commerciale, che l'individuo, però, elargisce senza troppa consapevolezza. A prescindere dal contenuto del GDPR, è stato affermato che le istituzioni europee ammetterebbero implicitamente l'esistenza di una logica commerciale nel trasferimento dei dati vista l'insistenza sulla presenza di un mercato del dato[120].

L'oggetto della tutela non è definito in modo univoco negli Stati Uniti e in Europa. Due studiosi americani hanno così approfondito la questione in modo analitico[121]. Le premesse giuridiche dei due ordinamenti sono inevitabilmente diverse, ma potrebbero essere riconciliate con riferimento alla nozione di dato personale[122]. A parere di chi scrive, si tratta di un'interessante opportunità comparatistica e di un approccio definitorio necessario, visto che il flusso dei dati è internazionale, non più tanto legato ai confini della nostra Unione Europea, e che se si vuole parlare di protezione del dato fin dalla progettazione, come di un principio ormai riconosciuto in tutto il mondo, bisogna capire cosa si intenda per "dato personale".

Negli Stati Uniti, spiegano, il diritto fornisce più definizioni di tale dato; su tutte primeggia la considerazione che un dato è personale se è davvero collegato ad una persona identificata. In contrasto, l'Unione Europea ha adottato un'unica definizione: il dato personale è qualsiasi informazione che identifica o potrebbe identificare uno specifico individuo in combinazione con altre informazioni, ossia anche indirettamente[123]. La riflessione sul concetto di dato personale ha coinvolto anche il Gruppo articolo 29, che nel 2007 ha adottato un parere[124], in cui si legge che è preferibile non restringere indebitamente l'interpretazione della definizione di dati personali, ma optare per la maggior flessibilità possibile nell'applicazione delle norme ai dati. Inoltre, il parere fornisce delle puntuali indicazioni, alle quali si rimanda, per esplicare

---

[119] J. M. VICTOR, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 *Yale L.J.* 513 (2013), 513: *"The EU's proposal includes three elements in particular that lend themselves to a property-based conception: consumers are granted clear entitlements to their own data; the data, even after it is transferred, carries a burden that "runs with" it and binds third parties; and consumers are protected through remedies grounded in property rules".*

[120] AIELLO, *La protezione cit.,* 445.

[121] P. M. SCHWARTZ, D. J. SOLOVE, *Reconciling Personal Information in the United States and European Union*, 102 *Cal. L. Rev.* 877 (2014).

[122] Questo è lo scopo di Schwartz e Solove nel paper citato.

[123] *Ibidem*, 879.

[124] Gruppo di lavoro articolo 29 per la protezione dei dati personali, Parere 4/2007 sul concetto di dati personali, 01248/07/IT, WP 136, adottato il 20 giugno 2007.

dettagliatamente e con esempi concreti le espressioni contenute nella definizione di dato: “qualsiasi informazione”, “concernente”, “persona fisica”, “identificata o identificabile”. Il nostro Garante per la Protezione dei Dati Personali conferma che sono oggetto tutelabile le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica[125]. Una criticità di una nozione tanto ampia di dato consiste nel rendere difficile l’opera di chi vuole ascrivere al novero dei diritti inviolabili la protezione di qualsiasi informazione riconducibile a un soggetto, perché vi è una grande disomogeneità tra le categorie dei dati suscettibili di protezione[126].

I due autori americani rilevano che la differenza considerabile appena riportata tra le due realtà giuridiche comporta significative difficoltà per l’armonizzazione dei due sistemi legali e dei costi rilevanti per le società e per il trasferimento internazionale dei dati[127].

A maggior chiarezza, Schwartz e Solove riportano la nuova definizione europea della proposta del 2012 (gli autori scrivono nel 2014, ma ad oggi possiamo invece aggiornare la definizione stessa, integrando il loro lavoro, visto che il testo del GDPR non si discosta da ciò che hanno scritto con riferimento alla proposta). Il GDPR recita all’articolo 4 che ai fini definitori si intende per dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Questa definizione si discosta da quella fornita nella direttiva 95/46 perché il focus non è più sulle parole “identificato-identificabile”, ma piuttosto su “direttamente-indirettamente”, e perché si ha l’aggiunta del riferimento all’identificativo online e all’identità genetica, ma in concreto la nozione si pone in continuità con la precedente. Il beneficio di questa scelta definitoria è che nulla scappa alla regolamentazione europea, a differenza delle lacune del sistema di tutela americano. Eppure, il contributo citato critica l’Unione nel non

[125] Sul sito del Garante: <http://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali;>.
[126] AIELLO, *La protezione cit.,* 439.
[127] SCHWARTZ, SOLOVE, *Reconciling cit.,* 879: *“The considerable divergence of the PII definitions in the United States and European Union poses significant difficulties for the harmonization of the two legal systems’ privacy regimes. These difficulties matter: the variation in legal definitions of PII raises compliance costs for companies who do business in both areas of the world. Additionally, the differing definitions threaten a status quo built around second-order mechanisms for allowing international data transfers”.*

trattare differentemente il dato che identifica da quello che potrebbe identificare la persona fisica[128].

Le norme definitorie degli Stati Uniti, si accennava, non offrono un'unica soluzione, ma si possono individuare tre approcci. Primariamente si ha l'approccio *tautological*: è personale qualsiasi informazione che identifica la persona. Il secondo è chiamato *nonpublic*, il quale esclude dalla protezione del dato personale le informazioni che sono pubblicamente accessibili o che statisticamente potrebbero esserlo. Infine, si riscontra nel diritto americano l'approccio per *specific-types* perché la norma, spesso uno *statute*, categorizza le informazioni che si considerano personali enumerandole semplicemente. In generale, però, si può affermare che negli Stati Uniti il dato tutelato è solo quello che identifica, non quello che potrebbe farlo e conseguentemente la tutela abbraccia meno fattispecie giuridiche rispetto all'Europa. Si deve allora optare per uno dei due approcci? Secondo l'opinione dell'articolo citato, è piuttosto pensabile un terzo modello definito *Personally Identifiable Information* 2.0 (PII 2.0), il quale riprende dagli Stati Uniti l'approccio basato sul danno arrecato, e la centralità del dato identificato, e dall'Europa la meritevolezza della tutela del dato identificabile. La chiave del nuovo modello è la costruzione di due diverse categorie di dato, identificato e identificabile, che siano disciplinate in modo differente a livello normativo e parametrate sulla base del rischio concreto di identificabilità. Il dato personale sarà tutelato diversamente a seconda del rischio di identificazione del soggetto a cui è riferito, il che comporta un incentivo per il titolare del trattamento ad anonimizzare il dato o quantomeno a renderlo solamente identificabile. A ciò consegue una maggiore tutela, quanto meno per la presenza di un incentivo, forma oggi inedita per il panorama europeo[129] .

---

[128] *Ibidem*, 887: *"The breadth of the EU approach has both benefits and drawbacks. The primary benefit is that hardly anything escapes EU privacy regulation. There are few gaps and inconsistencies under the EU approach, a stark contrast to the U.S. approach where such gaps and inconsistencies are legion. But there is also a primary drawback to the EU approach. Under both the Directive and Proposed Regulation, information is treated as the same whether it refers to an identified individual, or one who can be "indirectly identified"—that is, someone who the Directive terms "identifiable." All these terms constitute personal data, and their presence activates the "on" switch for triggering a full suite of obligations and protections. Yet, a broad continuum of identifiable information exists, and it includes different types of anonymous or pseudonymous information. Moreover, different levels of effort are required to identify information, and various risks are associated with the possible identification of data. Placing all such data into the same conceptual category as "data that currently relate to an identified person" lacks nuance. It also risks activating burdensome regulations for data-processing entities that are incommensurate with actual risks to the privacy of individuals".*

[129] *Ibidem*, 916: *"Therefore, for the goal of protecting privacy, it is far preferable to keep data in identifiable rather than identified form. PII 2.0 encourages keeping data in this format, while the EU approach to PII discourages keeping data merely identifiable. For these reasons, PII 2.0 would strengthen privacy protection in the European Union and resolve some of the ambiguities of EU data protection law".*

Continuando a riflettere in ambito mondiale, il primo accordo internazionale su principi condivisi in materia di privacy è rappresentato dalle Linee Guida Privacy OCSE[130], pubblicate nel 1980[131] e oggi aggiornate con il *OECD Privacy Framework* del 2013. Nel 1980 l'Organizzazione per la cooperazione e lo sviluppo economico riteneva che la definizione di dato personale spettasse a ciascuno stato membro, ma che in principio il dato riguardasse delle informazioni che direttamente o indirettamente potevano connettere ad una persona fisica[132]. Nel 2013 l'organizzazione, specificando che le nuove linee guida si applicano ai dati personali, sia del settore pubblico sia del privato, che per come sono trattati o per la loro natura o il contesto in cui sono utilizzati, pongono un rischio per la privacy e le libertà individuali[133], ribadisce la difficoltà nel definire compiutamente l'oggetto della tutela, pur investendo molte parole sul tema del trasferimento transfrontaliero dei dati e quindi sulla circolazione a livello mondiale degli stessi.

Ciò che si auspica, a questo punto, in prospettiva *de iure condendo*, è la creazione di un'unica definizione di dato personale a livello internazionale o una definizione comune ai vari ordinamenti, in modo da garantire, almeno su questo punto, uniformità e una tutela certa ed effettiva delle stesse situazioni.

Nel prossimo paragrafo si approfondirà la stretta relazione tra privacy e sicurezza per chiarire in ultimo punto il contesto in cui può utilmente inserirsi il principio della tutela del dato fin dalla progettazione.

6. Privacy vs. security, privacy and security

Prima di concludere queste prime pagine, è opportuno riflettere sul binomio privacy e sicurezza. Sempre l'Organizzazione per la cooperazione e lo sviluppo economico inserisce tra i principi del Framework del 2013 *Security Safeguards Principle* stabilendo che: *"personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised*

[130] The Organisation for Economic Cooperation and Development (OECD).
[131] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, in the form of a Recommendation by the Council of the OECD, 23 september 1980.
[132] Linee guida Privacy OCSE, versione del 1980, Cfr. Paragrafo 41, in commento alle definizioni contenute nelle Linee guida: "*The terms "personal data" and "data subject" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (e.g. a civil registration number) or indirect linkages (e.g. an address) may be connected to a particular physical person"*.
[133] OECD, Annex 2013, Guidelines governing the protection of privacy and transborder flows of personal data, Part One, General, Scope of Guidelines: *"These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties".*

access, destruction, use, modification or disclosure of data". La sicurezza, insomma, viaggia di pari passo con la privacy, ma la relazione tra questi due concetti è ambigua[134].

L'information security, espressione con cui si intende l'insieme delle attività che hanno come scopo la garanzia della protezione delle informazioni elettroniche dai possibili attacchi dolosi o colposi[135], è un aspetto necessario della protezione della privacy. È stato ritenuto che senza sufficiente sicurezza il diritto alla protezione dei dati diventerebbe un'illusione e le sue regole delle proclamazioni senza significato[136]. In più, lo stesso autore, ha sostenuto che è difficile descrivere le misure di sicurezza attraverso regole giuridiche, ma, bisogna ammettere, è solo lo strumento legale a poter indicare ciò che deve essere fatto in ambito di sicurezza[137]. La norma può fissare il principio generale e la prassi applicativa del tecnico la può implementare.

Le misure di sicurezza possono essere di tipo fisico, come la predisposizione di chiavi di sicurezza, allarmi, o di depositi blindati, organizzative, creando delle richieste di autorizzazioni all'accesso dei file o programmando delle procedure specifiche con obblighi e responsabilità e informazionali (come la scrittura cifrata).

Già con la legge n. 675/96 il legislatore aveva disposto l'adozione di misure di sicurezza per la protezione dei dati personali, ma solo con il Codice Privacy si ha una disciplina organica e innovativa. Il Titolo V del Codice è dedicato alla "Sicurezza dei dati e dei sistemi" e contiene la disciplina sia delle misure di sicurezza in generale sia le misure minime per specifici trattamenti. Il trattamento dei dati deve essere compiuto con idonee e preventive misure di sicurezza, tra cui sistemi di autenticazione e di autorizzazione per gli strumenti elettronici, al fine di custodire e controllare i dati riducendo al minimo i rischi di distruzione o perdita, di accesso non autorizzato o trattamento non consentito o non conforme alla finalità, tenendo come riferimento le conoscenze tecniche e la natura dei dati e le caratteristiche del trattamento[138]. Una misura importante è il Documento Programmatico sulla sicurezza, il quale deve essere redatto dal titolare del trattamento e aggiornato costantemente, secondo le modalità del Disciplinare tecnico in materia di misure minime di sicurezza, allegato B del

---

[134] GUARDA, *Data Protection cit.,* 68.

[135] La definizione è contenuta in C. RABAZZI, *Regole sulla sicurezza dei dati nel recente "codice sulla privacy"*, in *Ciberspazio e Dir.*, 2003, fasc. 3-4, 336.

[136] P. BLUME, *It is time for tomorrow,* cit., 7.

[137] *Ibidem*, 7.

[138] Cfr. Art. 31, D. lgs. 196/2003: "*1. 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*".

Codice[139]. Il D.P.S. è un piano di sicurezza annuale (con data certa cadenzata al 31 marzo), molto dettagliato, contenente le misure adottate dall'impresa o dall'ente pubblico e ha la funzione di provare l'adeguata adozione delle misure in previsione dei rischi del trattamento che verrà effettuato. Questa previsione del codice è idonea a fornire delle garanzie nel trattamento dei dati, ma, come è ovvio, genera dei costi rilevanti per le imprese. Gli oneri amministrativi legati alla privacy sono stati oggetto di una misurazione da parte della Scuola Superiore della Pubblica amministrazione, ed è emerso che il totale dei costi per il sistema delle piccole e medie imprese italiane ammonta a 2,19 miliardi di euro[140]. Nel 2005 è stato creato un nuovo strumento per la gestione della sicurezza delle informazioni: lo standard ISO 27001. Si tratta di una norma prevista dall'*International Standardization Organization*, che stabilisce i possibili requisiti di un sistema di gestione[141] e crea un nuovo strumento certificatorio che può essere implementato in combinazione con le misure del Codice, interessandosi in più della questione dei dati di business dell'organizzazione[142].

Il Documento Programmatico per la Sicurezza ha subito un profondo cambiamento nel 2008, su impulso del Garante per la protezione dei dati personali, che ha pubblicato il testo di Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali, in G.U. n. 287 del 9 dicembre 2008. Con il D.L. 25.6.2008, n. 112 il Governo ha provveduto a modificare il novero dei soggetti che sono tenuti all'adozione ed all'aggiornamento del D.P.S.: i soggetti che si limitano a trattare i soli dati personali non sensibili, eccetto quelli inerenti lo stato di salute o malattia dei propri dipendenti, ma senza l'indicazione della relativa diagnosi, sono tenuti a redigere una semplice autodichiarazione sostitutiva, con l'obbligo però di adottare tutte le misure di sicurezza necessarie e lo svantaggio di non avere più un ottimo strumento probatorio in presenza di un problema[143]. Ciò non è una questione di poco conto vista la responsabilità penale del titolare in caso di mancata adozione delle misure minime di sicurezza, ai sensi dell'articolo 169 comma 1 del Codice[144].

In realtà la parola "sicurezza" nella normativa italiana è utilizzata in due accezioni: sia per la necessità di tutelare i dati personali, a cui si fa riferimento sopra, sia per la garanzia di riservatezza, sia per l'individuazione degli interessi

---

[139] RABAZZI, *Regole sulla sicurezza cit.*, 344.

[140] Molto interessante la riflessione sui costi in DENTE, LUGARESI, RIGHETTINI, (a cura di), *La politica della privacy cit.*, 227-237.

[141] F. DI RESTA, *La tutela dei dati personali nella società dell'informazione*, con il contributo di A. BRUN e F. PIZZETTI, Giappichelli, Torino, 2009, 85.

[142] *Ibidem*, 87.

[143] M. MAZZEO, *Privacy: finisce l'era del D.P.S.*, in *Obbl. Contr.*, 2008, fasc. 8-9, in Leggi d'Italia.

[144] Cfr. Art. 169, co. 1, così modificato dall'art. 44, comma 9, lett. a), del decreto legge 30 dicembre 2008, n. 207 convertito, con modificazioni, dalla legge 27 febbraio 2009, n. 14.: "*Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni*".

la cui tutela può consentire una protezione minore della privacy, a vantaggio della sicurezza nazionale e pubblica[145]. Si parla di sicurezza nazionale quando si è costretti a bilanciare la protezione dei dati personali e la protezione contro la criminalità e il terrorismo. È inappropriato confrontare la privacy e la sicurezza in termini generali, è più giusto distinguere in base alla tipologia di sicurezza che si vuole ottenere, visto che la prevenzione dai reati è un ambito in cui le interferenze sulla privacy sono meno giustificabili rispetto alla sicurezza del Paese[146]. Tuttavia, le argomentazioni utilizzate dall'opinione pubblica americana di rinuncia favorevole a un "pizzico" di privacy per una maggiore sicurezza o di disinteresse nel non preoccuparsi della sorveglianza se non si ha nulla da nascondere (*"if you've got nothing to hide, you shouldn't worry about government surveillance")* sono state strenuamente condannate da studiosi americani, tra cui Daniel Solove, il quale ha cercato di dimostrare che il punto concettuale non è il "quantitativo di privacy*"* a cui si è disposti a rinunciare a favore della sicurezza sociale, ma la modalità con cui si possono proteggere i diritti senza dover per forza avvantaggiare le pratiche lesive della propria sfera di intimità[147].

A questo proposito si potrebbe citare un'intervista pubblicata sulla Stampa online nell'agosto 2016[148], in cui Giovanni Buttarelli, Garante europeo della protezione dei dati (G.E.P.D.), alla domanda se si dovesse pagare un prezzo in termini di privacy per facilitare la guerra al terrorismo, ha risposto che non ne vedeva l'utilità e che oggi possono essere sfruttati altri strumenti o escogitate

---

[145] PASCUZZI, *Il diritto dell'era digitale,* cit., 65. Si veda anche il capitolo *"dal diritto alla riservatezza alla computer privacy*" in PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., 57.

[146] Un'approfondita analisi in tema di sicurezza è offerta da S. S. BOURDILLON, *Privacy vs security… Are we done yet?,* in S. S. BOURDILLON, J. PHILLIPS, M. D. RYAN (a cura di), *Privacy vs Security*, Springer, 2014, 62: *"It is therefore inappropriate to try to oppose the values of privacy and security in general terms. Going further it is crucial to precisely identify the type and seriousness of the security threat at stake in order to properly identify the needs of the democratic society implicated. In this line it becomes necessary to distinguish, to the extent possible, between different, though closely related, concepts and in particular between the concepts of national security, public security and the prevention of crimes. Indeed, when "only" the prevention of crimes is at stake it should be more difficult to justify interferences to the right to respect of private life"*.

[147] Un'analisi completa del rapporto privacy-security si ha in D. J. SOLOVE, *Nothing to hide: the false tradeoff between privacy and security*, *Introduction*, Yale University Press, New Haven, 2011, 3: *"I propose to demonstrate how privacy interests can be better understood and how security interests can be more meaningfully evaluated. I aim to refute the recurrent arguments that skew the privacy-security debate toward the security side. I endeavor to show how the law frequently fixes on the wrong questions, such as whether privacy should be protected rather than how it should be protected. Privacy often can be protected without undue cost to security. In instances when adequate compromises can't be achieved, the tradeoff can be made in a manner that is fair to both sides. We can reach a better balance between privacy and security. We must. There is too much at stake to fail".* In cui tra l'altro è presente la storia della sorveglianza negli Stati Uniti.

[148] L'intervista è reperibile sul sito della Stampa all'indirizzo seguente: <http://www.lastampa.it/2016/07/31/esteri/il-garante-ue-inutile-limitare-la-privacy-prima-deve-migliorare-lantiterrorismo-j3JYDCwI0VPJWGymWDhLmI/ina.html>.

altre soluzioni. Il garante italiano Antonello Soro, sempre in una recente intervista sulla Stampa[149], è risultato dello stesso avviso: il diritto alla libertà individuale e alla sicurezza vanno bilanciati, senza arrivare ad un vantaggio eccessivo di uno dei due fronti. In questo senso il controllo generalizzato e invasivo, sullo stile statunitense, è condannabile. Appare agli occhi di molti e dell'opinione pubblica che la sicurezza sia in guerra con la privacy. Tuttavia questo negative-sum (privacy vs. security) può essere trasformato in un positive-sum, un win/win model (privacy and security), grazie ad un nuovo approccio proattivo, che sta prendendo piede in materia in questi ultimi anni, la privacy by design[150].

Non si può a questo punto dimenticare che il GDPR ha fissato nuove regole legate al tema della sicurezza, e ha codificato finalmente i principi di privacy by design e privacy by default, di cui si dirà ampiamente, e ha disciplinato nella Sezione 2 del Capo IV dedicata interamente alla sicurezza dei dati personali, la sicurezza del trattamento[151], la notifica di una violazione dei dati personali all'autorità di controllo[152] e la comunicazione di una violazione dei dati personali all'interessato[153]. È anche necessaria, a partire dall'adozione del regolamento, la predisposizione del documento di valutazione di impatto nel trattamento dei dati, o Privacy Impact Assessment, che consiste in un'analisi

[149] L'intervista è reperibile sul sito della Stampa al seguente indirizzo: <http://www.lastampa.it/2016/08/01/italia/cronache/il-garante-della-privacy-soro-i-controlli-di-massa-inefficaci-necessario-selezionare-i-bersagli-xxnC4MO5XBHENIurp4EalL/ina.html>.

[150] A. CAVOUKIAN, *International council on global privacy and security, by design*, Unintended Consequences of Technology, IEEE Potentials September/October 2016, 43-46.

[151] Cfr. Art. 32 "Sicurezza del trattamento" GDPR: "*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; 4.5.2016 L 119/51 Gazzetta ufficiale dell'Unione europea IT b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4.Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

[152] Cfr. Art. 33 "Notifica di una violazione dei dati personali all'autorità di controllo" GDPR.

[153] Cfr. Art. 34 "Comunicazione di una violazione dei dati personali all'interessato" GDPR.

del rischio del trattamento[154]. La suddetta analisi verrà effettuata prima dell'inizio del trattamento e sarà aggiornata costantemente, come era pensato il documento programmatico sulla sicurezza originariamente previsto dalla normativa italiana[155].

Attraverso il GDPR si assisterà alla armonizzazione europea in materia di sicurezza dei dati, molto vantaggiosa per i titolari e gli incaricati del trattamento. In ambito di sicurezza delle reti e dei sistemi informativi nell'Unione Europea è stata anche adottata la direttiva 2016/1148 del 6 luglio 2016 per un livello comune elevato di sicurezza informatica[156].

Un modo per garantire la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, così come definita dall'articolo 32 del GDPR, è implementare nel software o nell'hardware le regole giuridiche, così come accade nelle procedure di pseudonimizzazione e di cifratura dei dati personali. In questo senso, si può leggere anche l'importante principio di necessità nel trattamento dei dati, contenuto nel Codice Privacy. Il principio di necessità, che è stato una vera e propria innovazione italiana in tema di regolazione della privacy[157], all'articolo 3 recita*: "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".* La minimizzazione dell'uso dei dati personali e identificativi può essere inserita nella configurazione del sistema informatico, nella sua architettura, a vantaggio di una maggiore sicurezza dei dati, aspetto che è imprescindibile per la loro tutela effettiva ed efficace. Un esempio di questo approccio sono le privacy enhancing technologies, le quali hanno come scopo la tutela della riservatezza nel cyberspazio sfruttando gli strumenti della tecnologia stessa. Si tratta di tecnologie di rafforzamento della tutela della vita privata (PET), di vario tipo, come il ripristino automatico dell'anonimato dopo un determinato periodo di tempo. La Commissione Europea nel 2007 ha pubblicato un memorandum in

[154] Cfr. Art. 35, co. 1 "Valutazione d'impatto sulla protezione dei dati" GDPR: "*Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*".

[155] Già si annunciava in A. MANTELERO, *Riforma della direttiva comunitaria sulla Data Protection e Privacy Impact Assessment, Verso una Maggiore responsabilità dell'autore del trattamento?,* in *Dir. informazione e informatica*, 2012, fasc. 1, 148.

[156] Direttiva 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[157] GUARDA, *Data Protection cit.,* 85.

cui ha ritenuto che un più ampio uso delle PET rafforzerebbe la tutela della privacy, contribuirebbe all'ottemperanza delle norme sulla protezione dei dati e sarebbe complementare al quadro giuridico e ai meccanismi di attuazione vigenti[158].

Il futuro è l'incorporazione delle regole, ma anche dei valori, dei principi e dei codici di condotta all'interno del design[159], la prospettiva è quella in cui *"la tecnologia incorpora la regola"*[160].

[158] Commissione Europea, Tecnologie di rafforzamento della tutela della vita privata (PET), Il quadro giuridico vigente, MEMO/07/159, Bruxelles, 2 maggio 2007. Inoltre la Commissione ritiene: *"Per conseguire l'obiettivo di rafforzare il livello di protezione della privacy e dei dati nella Comunità, la Commissione intende intraprendere le seguenti iniziative: - identificare la necessità di tecnologie PET e definirne i requisiti tecnologici; - finanziare la ricerca nel settore delle PET: l'Europa, nell'ambito del suo VI programma quadro (2002-2006), ha erogato stanziamenti per un importo superiore a 18 milioni di EUR a favore della ricerca nel settore PET, e per i prossimi anni è previsto un rafforzamento sostanziale di tale dotazione; - promuovere l'uso delle PET da parte dell'industria; - garantire il rispetto di norme adeguate per la protezione dei dati mediante tecnologie PET (grazie a un'attività di normazione e coordinamento delle norme tecniche nazionali sulle misure di sicurezza applicabili al trattamento dei dati); - sensibilizzare i consumatori; - far sì che i consumatori possano operare una scelta con cognizione di causa grazie ai marchi di certificazione (Privacy seal). Questo ambito di azione sarà quindi implementato dalle politiche europee"*.

[159] GUARDA, *Data Protection cit.,* 68: *"The next step is to incorporate values, principles and codes of conduct inside the designs, in order to make clearer the necessary interaction between the technology development and the aims pursued by our legal systems*".

[160] PASCUZZI, *Il diritto dell'era digitale,* cit., 81.

Capitolo 2: La privacy by design

"L'attenzione rinnovata
per la protezione dei dati personali si conferma così
non solo come un'utopia necessaria,
ma come una via che deve essere percorsa
per mantenere condizioni di libertà della persona
e garantire condizioni di esercizio democratico del potere".
Rodotà, Il diritto di avere diritti, 2012.

1. Le origini dell'approccio e la sua affermazione

La Direzione Generale della Commissione Europea per la Giustizia e i Consumatori nel glossario del portale dedicato all'*european justice* definisce la privacy by design con le seguenti parole*: "(privacy by design) aims to build privacy and data protection upfront, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles"*[1]. Questa esplicazione è il risultato di un processo ventennale di elaborazione dottrinale che ha avuto inizio negli anni novanta, non in Europa, ma oltreoceano, in Canada, e che oggi ha condotto ad una formulazione positiva di questo approccio innovativo nel GDPR. Al fine di riflettere sull'incorporazione delle regole in materia di privacy nelle barriere architettoniche della tecnologia è opportuno tracciare la storia di questa metodologia attraverso i momenti chiave che la contraddistinguono.

[1] European Commission Directorate General for Justice and Consumers, Glossary in the portal of Justice, definition of *privacy by design*, last update 24 september 2015: <http://ec.europa.eu/justice/glossary/index_en.htm>. In merito alla Direzione Generale si veda della Commissione europea (JUST): <http://ec.europa.eu/justice/mission/index_it.htm>. Questa Direzione Generale è composta al suo interno da altre cinque direzioni: giustizia civile, giustizia penale, diritti fondamentali e cittadinanza dell'Unione, uguaglianza e consumatori, ha lo scopo di costruire uno "spazio europeo di giustizia" e più in generale rappresenta una delle trentatré direzioni in cui è suddivisa la Commissione Europea. In particolare, ogni direzione si occupa di uno specifico settore di cui si deve interessare la Commissione durante il proprio operato, ed è controllata da direttore generale (che a sua volta è sottoposto ad un commissario, attualmente individuato in Věra Jourová), con il fine di elaborare nuove proposte legislative, così favorire il lavoro dei commissari e organizzare eventi di sensibilizzazione dei cittadini europei, in tutto ciò potendo disporre di un proprio portafoglio.

1.1. La riflessione di Ann Cavoukian e i sette principi della privacy by design

Come si accennava, il concetto di privacy by design è stato inizialmente elaborato in Canada durante l'ultimo decennio del secolo scorso, grazie alla riflessione di Ann Cavoukian, la quale è attualmente uno dei maggiori esperti mondiali in materia di privacy. Ann ha ricoperto il ruolo di Information and Privacy Commissioner dell'Ontario (d'ora in avanti: IPC) dal 1997 al 2014, per l'eccezionale durata di tre mandati. L'IPC è l'autorità indipendente che si occupa della tutela della privacy in quella regione canadese, con la funzione di ufficio legislativo, consultivo, decisionale e promozionale, così come è stabilito dal *Freedom of Information and Protection of Privacy Act* del 1990, che è un *revised statute* consolidato in materia di protezione dei dati personali emanato dal Governo dell'Ontario, ancora oggi vigente[2]. Nel 2014, poi, è stata nominata Executive Director of Privacy And Big Data Institute della Ryerson University, sempre in Ontario, a Toronto, iniziando ad occuparsi di ricerca anche in ambito universitario e continuando a dare impulso ad una diffusione mondiale del suo pensiero. Questo istituto è un centro d'eccellenza che persegue e promuove una formazione interdisciplinare, che sia frutto di una ricerca critica e innovativa, la quale raccoglie studenti, docenti, di vari dipartimenti, e anche partners esterni, in modo da garantire una visione d'insieme e dei risultati concreti che possano essere impiegati, perché no, nelle iniziative commerciali delle aziende[3]. L'approccio interdisciplinare offerto dalla Ryerson University coglie appieno le poche parole proposte sul tema nel secondo paragrafo del precedente capitolo e dimostra ancora una volta l'importante ricchezza

[2] No. 4 (1), Part I Administration, Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, "Information and Privacy Commissioner": *"There shall be appointed, as an officer of the Legislature, an Information and Privacy Commissioner to exercise the powers and perform the duties prescribed by this or any other Act. R.S.O. 1990, c. F.31".* I poteri del Commissario sono elencati nel No 59, Part V, "Powers and duties of Commissioner": *"The Commissioner may, (a) offer comment on the privacy protection implications of proposed legislative schemes or government programs; (b) after hearing the head, order an institution to, (i) cease collection practices, and (ii) destroy collections of personal information, that contravene this Act; (c) in appropriate circumstances, authorize the collection of personal information otherwise than directly from the individual; (d) engage in or commission research into matters affecting the carrying out of the purposes of this Act; (e) conduct public education programs and provide information concerning this Act and the Commissioner's role and activities; and (f) receive representations from the public concerning the operation of this Act. R.S.O. 1990, c. F.31, s. 59".*

[3] Si veda il sito del Privacy and Big Data Institute della Ryerson University: <http://www.ryerson.ca/*pbd*i/about/exec_message/>: *"The Privacy and Big Data Institute, will pursue and promote critical interdisciplinary education, training, research, innovation, commercialization and related activities in Privacy and Big Data. The Institute will bring together students, faculty and staff from departments and academic units within Ryerson, and initiate and strengthen collaboration with partners from outside Ryerson".*

ottenibile dall'incontro e dalla collaborazione tra soggetti muniti di un bagaglio culturale e formativo tra loro differente e differenziato.

A parere dell'autrice canadese, è intesa privacy by design (d'ora in avanti anche con l'acronimo: pbd), la realizzazione di un progetto che consideri la protezione dei dati personali e della riservatezza sin dal principio, a partire dalla creazione del prodotto o dell'esecuzione di un servizio. L'approccio è caratterizzato dall'adozione di misure proattive, con lo scopo di anticipare e prevenire le invasioni della privacy prima che accadano; per l'appunto la privacy by design non consente di attendere la materializzazione del rischio di invasione alla sfera giuridica del soggetto e non intende offrire rimedi successivi, ma mira alla prevenzione, ossia ad operare *"before-the-fact"*[4]*.* Al fine di rendere più chiara la metodologia proposta, Ann Cavoukian ha elaborato sette principi fondativi che reggono il suo sistema della privacy, che è concepito ponendo al centro la figura dell'utente. I sette principi proposti sono i seguenti[5]:

---

[4] A. CAVOUKIAN, *Privacy by design,* Information & Privacy Commissioner, Ontario, Canada, 2009, 1 in <www.privacybydesign.ca>: "*The privacy by design framework employs an approach that is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they appen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after".*

[5] *Ibidem,* 2. Le descrizioni dei principi sono state tradotte per poterli esplicitare nel miglior modo possibile. Si è lavorato a partire dal documento del 2009 sopra citato e si è tenuto conto della sua revisione pubblicata nel settembre del 2013 sullo stesso sito riferito. Si è cercato di fornire delle parole equivalenti, ma non necessariamente uguali, per superare il rischio della tautologia dei concetti. Per completezza, ora si riporta l'elenco dei principi con le parole dell'autrice del 2009: *"1. Proactive not reactive: preventative not remedial: The Privacy by Design (Pbd) framework is characterized by the taking of proactive rather than reactive measures. It anticipates the risks and prevents privacy invasive events before they occur. Pbd does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to identify the risks and prevent the harms from arising. In short, Privacy by Design comes before-the-fact, not after. 2. Privacy as the default setting: We can all be certain of one thing — the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice, as the default. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual in order to protect their privacy — it is already built into the system, by default. 3. Privacy embedded into design: Privacy measures are embedded into the design and architecture of IT systems and business practices. These are not bolted on as add-ons, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is thus integral to the system, without diminishing functionality. 4. Full functionality: positive-sum, not zero-sum: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through the dated, zero-sum (either/or) approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have both. 5. End-to-end security: full lifecycle protection: Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely collected, used, retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end. 6. Visibility and transparency:*

1. *Proactive not reactive, Preventative not remedial* (Proattivo non reattivo, preventivo non correttivo). L'approccio è proattivo perché le misure in materia di privacy devono essere adottate nella fase di progettazione del prodotto tecnologico, per prevenire le violazioni e non doverne cercare un rimedio successivo. Il focus è anche sul ruolo giocato dalle scelte organizzative della direzione di un'azienda nel programma di protezione della privacy[6];
2. *Privacy as the Default Setting* (Privacy come impostazione predefinita). È necessario assicurare che i dati personali siano automaticamente protetti in ogni sistema ICT e in qualsiasi pratica commerciale, in modo che, anche quando non sia richiesta un'azione positiva da parte dell'individuo, la sua privacy sia protetta per impostazione predefinita. A questo proposito sono destinate varie tecnologie, tra cui quelle per la regolazione della geolocalizzazione, per l'anonimizzazione del segnale digitale e la crittografia del dato biometrico;
3. *Privacy Embedded into design* (Privacy incorporata nella progettazione). La privacy deve essere integrata nel design e così rappresentare un essenziale componente della funzionalità della tecnologia, essendo appunto inserita nella sua architettura;
4. *Full functionality – Positive-sum, Not zero-sum* (Massima funzionalità, valore positivo e non valore zero). Questo approccio intende soddisfare tutti gli interessi e gli obiettivi in gioco, dimostrando che non sempre è imposto scegliere a vantaggio di una singola posizione ed escluderne un'altra, come nel caso della relazione tra privacy e sicurezza;
5. *End-to-end security – full lifecycle protection* (Sicurezza fino alla fine, durante tutto il ciclo del prodotto o servizio). L'approccio deve essere mantenuto per tutta la durata del trattamento dei dati, affinché il dato sia

---

keep it open: Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. The data subject is made fully aware of the personal data being collected, and for what purpose(s). All the component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify! 7. Respect for user privacy: keep it user-centric: Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. The goal is to ensure user-centred privacy in an increasingly connected world. Keep it user-centric".

[6] A. CAVOUKIAN, *Operationalizing privacy by design: a guide to implementing strong privacy practices*, Information and Privacy Commisioner, Ontario, 2012, in <www.privacybydesign.ca>, 3: "*The focus is on the role played by organizational leadership/senior management in the formation, execution and measurement of an actionable privacy program. Research and case studies pertaining to the role of Boards of Directors, the definition of an effective privacy policy, the execution of a "Pbd Privacy Impact Assessment" (a truly holistic approach to privacy and privacy risk management) and a "Federated PIA," as well as a variety of other applications contribute to further implementation guidance".*

acquisito, trattenuto e distrutto in sicurezza e così la gestione dei dati sia conforme dall'inizio alla fine;

6. *Visibility and transparency – keep it Open* (Visibilità e trasparenza). La protezione deve essere verificabile dall'individuo grazie alla visibilità delle misure e alla loro trasparenza, nel senso che l'individuo può costantemente controllare che le operazioni sui suoi dati siano conformi alle previsioni e agli obiettivi;
7. *Respect for User Privacy – keep it User-Centric* (Rispetto per la privacy dell'utente, centralità dell'utente). La privacy by design richiede che l'utente, l'individuo, sia al centro, perciò devono essere implementate le misure di protezione per impostazione predefinita, la presenza di notifiche appropriate e delle opzioni di policy facili da utilizzare. Tutto ciò perché si deve assicurare la protezione dell'utente indipendentemente dalla sua partecipazione spontanea, ma con opzioni che la rendono in un certo senso obbligatoria[7].

Gli scenari applicativi considerati da Ann Cavoukian per la sua pbd sono principalmente tre, ossia la tecnologia dell'informazione, le pratiche commerciali e le strutture di rete. Questa trilogia coinvolge sia il settore pubblico, sia quello privato; si dovrebbe considerare la privacy by design non come la temuta assunzione di costi eccessivi per le aziende, ma come piuttosto un vantaggio in termini di competitività e farne perciò una questione di business e non di compliance[8].

La ricerca canadese sulla pbd ha consentito la produzione di molti articoli scientifici da parte di professionisti di varia formazione, tra i quali giuristi, informatici, economisti, o esperti di sanità, coinvolgendo così nove aree chiave di applicazione più concreta: la videosorveglianza, l'utilizzo di dati biometrici, i contatori e le reti intelligenti, i dispositivi mobili e quelli per le comunicazioni, le tecnologie di connettività wireless, le tecnologie per la memorizzazione automatica delle informazioni, il monitoraggio remoto dei pazienti con problemi sanitari e la gestione e l'analisi dei big data[9].

Inoltre, la già commissaria dell'IPC ha speso delle parole per dissipare tre miti sulla privacy molti diffusi ai giorni nostri. Innanzitutto, la privacy non è

---

[7] *Ibidem,* 4: *"The privacy interests of the end-user, customer or citizen are paramount. Pbd demands that application and process developers undertake a collection of activities to ensure that an individual's privacy is protected even if they take no explicit steps to protect it. Privacy defaults are key; clear notice is equally important. Especially within complex systems (e.g. contemporary Social Network Services), users should be provided with a wide range of privacy-empowering options".*

[8] CAVOUKIAN, *Privacy by design,* cit., 3.

[9] *Ibidem*, 5: *"9 Pbd Application Areas: CCTV/Surveillance cameras in mass transit systems; Biometrics used in casinos and gaming facilities; Smart Meters and the Smart Grid; Mobile Communications; Near Field Communications; RFIDs and sensor technologies; Redesigning IP Geolocation; Remote Home Health Care; Big Data and Data Analytics".*

morta, come alcuni vorrebbero far credere[10]. A suo parere, se ciò fosse vero, anche la libertà dovrebbe soccombere, ma ciò non è possibile perché la caratteristica prima dell'umanità è di essere libera. Secondariamente, non è attendibile affermare che nessuno si preoccupa più della propria privacy; infatti, ciascuno, per quanto sia sempre connesso e condivida sempre più informazioni, desidera preservare una anche minima sfera di riservatezza, che gli permetta di godere di momenti di solitudine e di intimità. Infine, non sarebbe possibile ritenere che aumentare la sicurezza significhi diminuire la privacy: la pbd intende proprio promuovere un valore positivo tra i due concetti, ovverosia un connubio tra i due valori, e ciò potrebbe davvero realizzarsi se si seguissero i sette principi fondativi citati. La protezione della privacy sarebbe, sempre secondo Ann Cavoukian, il fondamento della *freedom* e della *liberty* del nostro tempo[11]. Il lavoro della commissaria canadese è stato diffuso in tutto il mondo e tramite alla sua partecipazione agli eventi internazionali in tema di privacy si è giunti ad un riconoscimento formale della validità del principio di pbd nel 2010 a Gerusalemme.

1.2. La Resolution of Jerusalem e il riconoscimento internazionale del principio

Ogni anno dal 1979 si svolge una Conferenza Internazionale che vede come protagonisti i garanti della privacy e le autorità che si occupano della protezione dei dati in tutto il mondo: L'*International Conference of Data Protection and Privacy Commissioners.* Ad oggi si contano 76 membri accreditati, tra i quali il Consiglio d'Europa, l'Unione Europea, gli Stati Uniti d'America e l'Italia. Lo scopo perseguito è di dedicare uno spazio in cui le varie autorità possono collaborare in concerto, grazie ad una maggiore diffusione della conoscenza e al supporto delle altre realtà sparse nel mondo. La Conferenza mira ad essere un eccezionale forum globale, che crei nuova conoscenza, attraverso risoluzioni e dichiarazioni, che provveda all'assistenza pratica alle autorità, fornisca una direzione internazionale sulle questioni, connetta e supporti gli sforzi delle varie organizzazioni locali e regionali, in

[10] Nel 2010 a New York durante la conferenza "The Last Hope" l'investigatore privato Steve Rambam disse nel suo intervento: "*privacy is dead, get over it"*. Questo discorso fu molto diretto e provocatorio perché aveva il fine di dimostrare che l'utilizzo dei vari database per cercare le informazioni sugli individui non è un'attività così complessa come potrebbe apparire, anzi, a partire da un numero di telefono è possibile risalire facilmente ad ogni più dettagliata notizia che riguarda quella persona. Insomma, questo trend sarebbe impossibile da fermare, allora tanto vale smettere di pensarci.

[11] Nel Dizionario Cambridge inglese-italiano della Cambridge University Press edizione del 2016 si intende *freedom* come il diritto a vivere nel modo in cui si vuole senza essere controllati da chiunque altro ("*the right to live in the way you want without being controlled by anyone else*") e per *liberty* la libertà di vivere, lavorare e viaggiare come si desidera ("*the freedom to live, work, and travel as you want to*").

modo da aumentare la protezione dei dati e della privacy e aumentarne la promozione[12].

La trentaduesima Conferenza Internazionale ha segnato un punto di svolta per la pbd. Nell'ottobre del 2010 in Israele, a Gerusalemme, i commissari hanno riflettuto sulle problematiche presenti nell'era digitale e hanno elaborato la *Resolution on privacy by design*, ossia un testo condiviso che prende posizione sul tema e che definisce il carattere fondamentale della pbd, elevandola a principio di diritto internazionale. All'inizio del documento si affermano delle considerazioni preliminari: si ammette che il progresso tecnologico porta con sé dei cambiamenti per la privacy e per la capacità degli individui di esercitare effettivamente i loro diritti informativi, si accetta che la regolazione esistente non è sufficiente per salvaguardarli completamente e si intuisce che è necessario un approccio più robusto per rispondere ai crescenti e sistematici effetti delle tecnologie dell'informazione e della comunicazione e delle infrastrutture di rete (d'ora in avanti ICT)[13]. In aggiunta, si dichiara che l'incorporazione della privacy all'interno del design, delle operazioni e della gestione dei sistemi tecnologici per tutto il "ciclo di vita" delle informazioni è necessaria per proteggere pienamente la riservatezza e la protezione dei dati personali[14].

Il testo nella sua parte risolutiva statuisce tre punti condivisi dalle varie autorità. In primo luogo, è riconosciuto che la privacy by design è una componente essenziale della protezione della privacy. Poi è stabilito che le autorità intendono favorirne l'adozione attraverso i sette principi fondativi in modo che sia assunta generalmente come modello organizzativo e operazionale per impostazione predefinita; a questo fine vengono riproposti nel

[12] La missione è indicata sul documento ICDPPC *Rules and Procedures - Consolidated version (November 2016)* sul sito di riferimento della Conferenza <https://icdppc.org/document-archive/rules-procedures/>: *"1.1. The purposes of the Conference are: a. To promote and enhance internationally personal data protection and privacy rights; b. To improve data protection and privacy by providing a forum that encourages dialogue, cooperation and information sharing; c. To draft and adopt joint resolutions and declarations on subjects that warrant the common interest or concern of the accredited members, and promote their implementation; d. To be a meeting point between accredited members and other international fora or organisations that share common objectives; e. To encourage and facilitate cooperation and the exchange of information among accredited members, in particular regarding enforcement actions; f. To promote the development of international standards in the field of protection of personal data".*

[13] Le tecnologie dell'informazione e della comunicazione (ICT) sono l'insieme degli strumenti che consentono l'elaborazione, la trasmissione e la gestione delle informazioni nell'era digitale.

[14] Cfr. 32nd International Conference of Data Protection and Privacy Commissioners, *Resolution on Privacy by Design*, Jerusalem, Israel 27-29 October, 2010: *"Recognizing that embedding privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle, is necessary to fully protect privacy; Offering Privacy by Design as a holistic concept that may be applied to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure".*

testo i principi così come definiti dal Commissario Ann Cavoukian[15]. In terza posizione si invitano le autorità e i commissari stessi a promuovere la pbd per quanto possibile e a incoraggiarne l'incorporazione nelle privacy policies e, ancor più importante, nelle legislazioni degli ordinamenti di appartenenza, aumentando la ricerca proattiva sul principio e considerandolo nell'agenda per l'International Data Privacy Day[16]. Infine, si rimanda alla conferenza successiva, nella quale dovranno essere condivisi i risultati ottenuti e le pratiche implementate[17].

Questa risoluzione è stata proposta dalla stessa Cavoukian, ma ha riscosso molto successo alla Conferenza ed è stata sottoscritta all'unanimità da parte del resto dei commissari e delle autorità presenti. L'inserimento in una risoluzione del principio di privacy by design fa sì che l'attenzione mondiale delle autorità sia rivolta sul tema e che le stesse autorità si facciano sue promotrici. Si può dire che nel 2010 la riflessione si è trasferita da un livello dottrinale e programmatico ad un piano più organizzativo e legislativo. Insomma, la pbd non è rimasta un'intuizione innovativa di una commissaria d'oltreoceano, ma è diventata l'oggetto principale di una risoluzione vincolante in tutto il mondo, seppur limitata ai membri accreditati che l'hanno sottoscritta. È vero che la Conferenza Internazionale non è dotata di uno status legale definito, perché non è né un'organizzazione internazionale né uno luogo dedicato alla predisposizione di trattati vincolanti[18]. È innegabile però che si tratti di uno

---

[15] Cfr. Resolution*: "The Foundational Principles: Proactive not Reactive; Preventative not Remedial; Privacy as the Default; Privacy Embedded into Design; Full Functionality: Positive-Sum, not Zero-Sum; End-to-End Lifecycle Protection; Visibility and Transparency; Respect for User Privacy".*

[16] Il Consiglio d'Europa nel 2006 ha designato una data per celebrare la protezione della *privacy,* ossia l'*International Data Protection Day*, che si tiene ogni anno il 28 gennaio. La scelta è dovuta all'anniversario dell'apertura delle firme per la Convenzione del 28 gennaio 1981, n. 108, sulla protezione degli individui con riguardo al trattamento automatico dei dati personali, come si può leggere sul sito di riferimento dell'organismo interazionale <http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp>: *"On 26 April 2006, the Committee of Ministers of the Council of Europe decided to launch a Data Protection Day, to be celebrated each year on 28 January. Why the 28 January? This date corresponds to the anniversary of the opening for signature of the Council of Europe's Convention 108 for the Protection of individuals with regard to automatic processing of personal data which has been for over 30 years a cornerstone of data protection, in Europe and beyond. Data Protection Day is now celebrated globally and is called the "Privacy Day" outside Europe"*.

[17] Cfr. Resolution: "*3. Invite Data Protection and Privacy Commissioners/Authorities to: a. promote Privacy by Design, as widely as possible through distribution of materials, education and personal advocacy; b. foster the incorporation of the Privacy by Design Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions; c. proactively encourage research on Privacy by Design; d. consider adding Privacy by Design to the agendas of events taking place on International Data Privacy Day (January 28); e. report back to the 33rd International Data Protection and Privacy Commissioners Conference, where appropriate, on Privacy by Design activities and initiatives undertaken within their jurisdictions with a view to sharing best practices".*

[18] Cfr. ICDPPC Rules and Procedures*: "1. The Status of the Conference: The International Conference of Data Protection and Privacy Commissioners (the "Conference") is an entity in its*

strumento importante e propulsivo per lo sviluppo di approcci nuovi e metodologie alternative in materia di privacy. La Conferenza di Gerusalemme, infatti, è stata considerata una pietra miliare per l'inizio di un processo di condivisione del principio, tanto da condurre ad un suo successivo riconoscimento da parte della Federal Trade Commission degli Stati Uniti nel 2012, definendola una pratica fondamentale per proteggere oggi la privacy e da spingere la Commissione Europea ad inserirla nella Proposta del GDPR. Nel prossimo paragrafo si tratterà del Report *Protecting Consumer Privacy in an Era of Rapid Change* della Commissione statunitense e si proseguirà poi con la presenza del principio nella normativa europea.

1.3 Il Report della Federal Trade Commission per la protezione dei dati personali dei consumatori

La Federal Trade Commission (d'ora in avanti anche FTC) è un'agenzia federale degli Stati Uniti d'America che dal 1914 si occupa di prevenire le pratiche commerciali non concorrenziali, ingannevoli o sleali, per garantire la protezione dei consumatori[19]. Nel 2012 la FTC ha pubblicato un Report intitolato *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*. In questo documento si raccomandano tre principi per proteggere la privacy dei consumatori nell'era digitale: l'approccio *pbd* per le pratiche commerciali, la semplificazione delle scelte del consumatore sui propri dati e una maggiore trasparenza nel trattamento. Il testo ha lo scopo di indicare le migliori pratiche che le companies statunitensi dovrebbero implementare per garantire un'adeguata tutela del consumatore in forza di una regolamentazione interna. Le società coinvolte dal Report sono quelle che raccolgono e trattano i dati dei propri consumatori, a meno che il numero di questi sia limitato (meno di 5000 all'anno) e che i dati stessi non siano sensibili o non vengano mai condivisi con terze parti, sempreché siano tutte informazioni riferibili ragionevolmente ad un preciso soggetto, computer o device[20]. La FTC ha all'uopo elaborato un framework molto analitico e ha al contempo auspicato che il Congresso provveda alla

---

own right, representing the collective accredited members. For the purposes of this document, the term the Conference refers to the collective accredited members. There is no compelling need in the short-term to incorporate or otherwise give the Conference legal status. The legal status of the Conference can be revisited at a later date".

[19] Sul sito dell'agenzia sono indicati gli obiettivi prefissati <https://www.ftc.gov/>: *"To prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity"*.

[20] Cfr. Report, 22: *"The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties".*

redazione di una legislazione federale sulla privacy, utilizzando come linee guida il Report e rendendosi disponibile nel collaborare ai lavori legislativi[21]. In risposta a vari commenti critici giunti da varie società statunitensi sulla proposta di una legislazione federale, la FTC ha specificato che il documento ha soltanto lo scopo di incentivare le migliori pratiche adottabili e non di sostituire o entrare in conflitto con la disciplina già prevista dalle regole esistenti e dagli statutes[22]. A breve sarà riferito che in realtà è il problema della definizione della natura giuridica dei Report della FTC non è di poco conto.

Per quanto riguarda la privacy by design, la FTC ha statuito un principio di base e due finali. Innanzitutto, le società dovrebbero promuovere la privacy dei consumatori in ogni parte delle loro organizzazioni e ad ogni stadio dello sviluppo dei loro prodotti e servizi[23]. La pbd, a suo avviso, è un principio da supportare, tenendo presente l'esponenziale aumento del trasferimento dei dati a livello globale, soprattutto per sollevare il consumatore dall'incombenza di leggere e capire le lunghe e incomprensibili notifiche per il trattamento dei suoi dati e per evitargli scelte troppo difficili per le conoscenze possedute sull'argomento.

Successivamente l'agenzia ha indicato un principio finale definito "sostanziale": si richiede alle società di incorporare la protezione della privacy all'interno delle loro pratiche, tra le quali quelle per la sicurezza dei dati, per i limiti alla loro raccolta, per la conservazione e l'eliminazione in sicurezza e per l'accuratezza degli stessi[24]. La FTC, per esplicare ciò che ha inteso per "limiti nella raccolta dei dati", ha citato il caso del *Graduate Management Admission Council*, il quale ha sviluppato una tecnologia che impedisce un utilizzo ulteriore delle impronte digitali ricavate dai test di ammissione all'università americane se non per gli scopi specifici degli stessi test, così garantendo che le informazioni a dir poco identificative non siano confrontate con altri database, come quelli che riguardano i criminali[25].

---

[21] Cfr. l'executive summary del Report: "*The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation".*

[22] Cfr. Report, 16: *"However, the framework is meant to encourage best practices and is not intended to conflict with requirements of existing laws and regulations. To the extent that components of the framework exceed, but do not conflict with existing statutory requirements, entities covered by those statutes should view the framework as best practices to promote consumer privacy".*

[23] Cfr. Report, 22: *"Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services".*

[24] Cfr. Report, 23: "*Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy".*

[25] Cfr. Report, 27: *"One example of a company innovating around the concept of privacy by design through collection limitation is the Graduate Management Admission Council ("GMAC").*

Affinché la privacy by design sia davvero adottata la FTC ha proposto un ulteriore principio finale di tipo procedurale: le società dovrebbero mantenere una gestione sui dati di natura onnicomprensiva, ossia costante e adeguata per tutto il ciclo di vita dei loro prodotti e servizi[26]. Le companies in realtà dovrebbero disporre di un periodo di transizione; infatti si potranno inizialmente concentrare sui sistemi che contengono dati sensibili e solo in seguito dovranno predisporre le vere e proprie modalità organizzative onnicomprensive che garantiscano la protezione per ogni tipologia di dato e in ogni fase del suo trattamento.

L'agenzia statunitense ha inoltre deciso di focalizzarsi su cinque voci di azione applicativa per promuovere il suo privacy framework: la direttiva di controllo do not track per i siti web, i servizi di comunicazione mobile, la profilazione dei consumatori per fini commerciali da parte dei data brokers, la gestione dei dati nelle grandi piattaforme dei social media, dei browsers o degli internet service providers e l'applicabilità dei codici di condotta derivanti dall'autoregolamentazione[27]. Queste applicazioni sono per l'appunto alcune delle aree chiave in cui si violano abitualmente le regole a protezione della riservatezza.

A questo punto è interessante accennare al *dissenting statement* del Commissario J. Thomas Rosch, il quale, nell'appendice al Report, esprime le sue perplessità sulla natura giuridica delle raccomandazioni previste nel documento, *ivi* dichiarate semplicemente delle "best practices", ma che in realtà sarebbero vincolanti: il linguaggio utilizzato, l'indicazione di modello per una possibile legislazione e che la presenza di codici di condotta obbligatori, sarebbero indici del fatto che le pratiche, apparentemente lasciate all'autoregolamentazione, avrebbero invece natura obbligatoria; a suo avviso non noterebbe alcuna differenza da un atto legislativo del Congresso perché le

---

This entity previously collected fingerprints from individuals taking the Graduate Management Admission Test. After concerns were raised about individuals' fingerprints being cross-referenced against criminal databases, GMAC developed a system that allowed for collection of palm prints that could be used solely for test-taking purposes. The palm print technology is as accurate as fingerprinting but less susceptible to "function creep" over time than the taking of fingerprints, because palm prints are not widely used as a common identifier. GMAC received a privacy innovation award for small businesses for its work in this area".

[26] Cfr. Report, 32: *"Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services".*

[27] La direttiva di controllo do not track all'interno di un sito web consente all'utente di scegliere di non essere tracciato nelle sue ricerche. Difatti, molti siti tengono traccia del comportamento dei visitatori per vendere o cedere le informazioni ottenute a vari soggetti terzi, sfruttando le potenzialità economiche degli inserti pubblicitari. In realtà oggi la funzione antitracciamento è tendenzialmente garantita dalla maggior parte dei motori di ricerca e dai siti più visitati, anche se rimane discrezionale per il gestore osservare la scelta dell'utente. Proprio per questo la FTC preme molto sulla progettazione dei siti integrata con la previsione del servizio do not track.

società statunitensi si sentono forzate e veicolate nelle posizioni della FTC e nella sua direzione[28].

Parimenti, due autori statunitensi hanno riflettuto sulla problematicità della vincolatività o meno del contenuto del Report, spiegando che le società considerano davvero seriamente le indicazioni poste dalla FTC e con la conseguenza che, in alcuni casi, queste semplici raccomandazioni diventino delle vere e proprie regole, la cui natura di soft law, peraltro, potrebbe essere ritenuta analoga a quella di un'opinione di un giudice; quelle che dovrebbero essere delle semplici interpretazioni della commissione, stabilendo invece degli incentivi alle companies per la loro ottemperanza, finiscono per essere delle prescrizioni regolatorie[29]. Nello stesso contributo citato si ritiene perfino che la FTC stia creando nel tempo un corpo federale di regole di common law in materia di privacy. Da questa affermazione si può solo che dedurre l'importanza delle statuizioni della Commissione e da ciò la rilevanza che ha assunto la pbd in ambito statunitense vista la sua presenza in uno degli ultimi Report.

In un altro paper di un autore statunitense sulla privacy by design si è auspicato che, nell'attesa dell'emanazione di una legislazione federale, la FTC perseveri nel suo ruolo di promozione strategica e nell'incentivare l'autoregolamentazione tra le imprese, le cui scelte sono sì veicolate dall'analisi dei costi-benefici legata alle dinamiche del mercato, ma possono essere indirizzate dall'agenzia[30].

---

[28] Cfr. Appendix C del Report, C-8: *"Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than "best practices," I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement. The Report also acknowledges that it is intended to serve as a template for legislative recommendations. Moreover, to the extent that the Report's "best practices" mirror the Administration's privacy "Bill of Rights," the President has specifically asked either that the "Bill of Rights" be adopted by the Congress or that they be distilled into "enforceable codes of conduct." As I testified before the same subcommittee, this is a "tautology"; either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in which case there can be no pretense that they are "voluntary." It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the "best practices" or face the wrath of "the Commission" or its staff".*

[29] D. J. SOLOVE, W. HARTZOG, *The FTC and the new common law of privacy*, 114 *Colum. L. Rev.* 583 (2014), 626: "*Companies take the guidance in these materials seriously. In some cases, statements in these materials can become almost like rules. Perhaps the best analogue to this soft law is dicta in judicial opinions. The FTC materials do not have the same force and effect of a settlement; they are merely statements by the FTC about how it interprets its regulatory authority and Section 5, and how it might choose to enforce in the future. The FTC might change course or not enforce in that manner. The FTC might attempt an enforcement but be challenged by a company in court. Thus, FTC materials do not appear to be as strongly precedential as settlements, but they create incentives for companies to comply, and thus serve as a softer kind of rule*".

[30] In questo senso, I. S. RUBINSTEIN, *Regulating privacy by design*, 26 *Berkeley Tech. L.J.* 1409 (2011), 1453.

Ci si chiede allora se la FTC possa agire giudizialmente per proteggere la privacy dei consumatori sulla base del Report pubblicato, quindi anche per garantire l'implementazione della pbd. Ai sensi del Federal Trade Commission Act, l'agenzia può promuovere un'azione legale solo se gli atti delle società o le loro pratiche siano "*unfair or deceptive*". In materia di privacy si potrebbe agire sulla base del carattere ingannevole, ossia il secondo criterio, che emerge quando non si ha conformità tra quanto viene promesso dall'organizzazione e quanto viene concretamente fatto; tutto ciò comporta che la Commissione abbia delle possibilità legali effettive molto limitate e che in soccorso al consumatore residui solo la tradizionale tutela prevista dalla legislazione statunitense[31]. Come si vedrà, però, i più recenti orientamenti dell'agenzia prevedono anche l'utilizzo del primo criterio di *unfair*, consentendo una tutela di fronte ad un design scorretto di un prodotto informatico.

Si può dunque citare il commento al framework esposto dalla Commissaria dell'FTC Edith Ramirez durante la *Privacy by Design Conference* di Hong Kong nel 2012, tenutasi poco dopo la pubblicazione del Report[32]. Premettendo che la pbd è il concetto che genera molto fermento, l'autore della relazione ritiene che "*respecting privacy must be considered integral to the innovation process*"[33]. La Commissaria spiega che si ha una vera e propria urgenza nel servirsi di questo approccio a causa della quasi costante raccolta e diffusione dei dati dei consumatori, resa possibile dai cambiamenti tecnologici[34]. L'intento della FTC è di far sì che la privacy dei fruitori dei prodotti e dei servizi non dipenda dalla loro capacità di leggere e capire le policies, ma dalla previsione di garanzie a monte, tali per cui il diritto sia una sicurezza, vale a dire sia realmente garantito. Tutto ciò dovrebbe valere sia per gli Stati Uniti che per i processi di circolazione dei dati dei consumatori in tutto il mondo attraverso i

[31] La spiegazione è offerta in materia di tracciamento, ma vale in generale da parte di M. JENNINGS, *To track or not to track: recent legislative proposals to protect consumer privacy*, 49 *Harv. J. on Legis*. 193 (2012), 196-197: *"Under the basic consumer protection provision of the FTC Act, the FTC can only take action if a company's acts or practices are "unfair or deceptive." The FTC's jurisdiction over "unfair" acts or practices includes those that unfairly cause injury or a reasonable likelihood of injury. The typical Internet privacy case does not fit neatly within this unfairness jurisdiction. For a practice to be deceptive, a company must have promised one thing and then done another. For example, if a company promised certain protections in its privacy policy and breached that promise, the FTC would have jurisdiction to bring suit against the company. Although the FTC has found limited ways to adapt the current framework to address privacy concerns, its commissioners believe that comprehensive data privacy legislation would better protect consumers".*

[32] E. RAMIREZ, *Privacy by design and the New Privacy Framework of the U.S. Federal Trade Commission,* Remarks of Commissioner in the *Privacy by Design Conference*, Hong Kong, June 13, 2012. Il commento è facilmente reperibile sul sito della FTC: <https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf>.

[33] *Ibidem,* 2.

[34] *Ibidem,* 3: *"But it has greater urgency as a result of the nearly constant collection and sharing of consumer data that changes in technology have made possible".*

c.d. trasferimenti transfrontalieri. Il messaggio conclusivo della Commissaria coglie una questione vitale e spinosa per la pbd, tanto da dover riportare le sue stesse parole:

> *"But ingraining a culture of privacy is not something governments can impose by fiat. As regulators, we can advocate privacy by design as a best practice; we can mandate comprehensive privacy programs in our orders; and we can encourage privacy by design through voluntary international regimes. But it is ultimately up to businesses to ensure that privacy by design is more than a slogan. I am encouraged by the efforts of many organizations to incorporate privacy by design, and I am hopeful we will see this more and more"*[35].

Insomma, sta alle società e ai soggetti commerciali provvedere in modo che la privacy sia tutelata by design. Tuttavia la cultura della privacy non potrà mai essere imposta solo dai governi, ma dovrà maturare nelle società dell'informazione ed essere sempre più incoraggiata dagli esperti del settore.

La pbd potrebbe essere inserita nella futura legislazione statunitense, grazie ai continui sforzi della FTC e come si approfondirà nel terzo capitolo.

Nei prossimi paragrafi, invece, si concentrerà lo sguardo in Europa per tracciare la storia della presenza del principio a partire dalla proposta della Commissione Europea per il nuovo regolamento in materia di protezione dei dati personali.

1.4. La Proposta della Commissione Europea e l'avvento del GDPR

Il 2012 si è rivelato un anno decisivo per la privacy by design perché la FTC ha pubblicato il Report citato nel precedente paragrafo e la Commissione Europea ha inserito questo approccio nella sua proposta di regolamento, come si è accennato nel precedente capitolo. In questo paragrafo si intende tracciare il percorso del principio negli anni di elaborazione del GDPR.

All'interno della prima documentazione, la Commissione asserisce che la protezione dei diritti e delle libertà dei soggetti con riguardo al trattamento dei dati personali richiede che siano assunte appropriate misure tecniche e organizzative sia al momento della progettazione del processo sia in quello del processo stesso per assicurare il rispetto dei requisiti del Regolamento; affinché si garantisca e si assicuri questa conformità, il titolare del trattamento dovrebbe quindi adottare delle politiche interne e implementare delle misure appropriate,

[35] *Ibidem*, 10.

che incontrino in particolare i principi di data protection by design and data protection by default[36].

A tal proposito, l'organo esecutivo dell'Unione Europea richiede che gli siano conferiti maggiori poteri per assicurare uniformi condizioni di implementazione della nuova regolazione e per poter definire degli standard in relazione alla responsabilità del titolare del trattamento per la protezione dei dati by design e by default e per la documentazione che deve presentare[37].

Venendo al cuore della proposta, nella prima sezione si fissa all'articolo 22 la responsabilità del controller: questo soggetto dovrà adottare delle politiche e implementare delle misure appropriate per assicurare ed essere in grado di dimostrare che il trattamento sia conforme al Regolamento[38].

Nella norma che segue si inserisce in modo esplicito, per la prima volta, la protezione dei dati personali by design e by default. Ebbene, all'articolo 23 si stabilisce che, considerando lo stato dell'arte e i costi di implementazione, il titolare stesso dovrà, sia al momento della determinazione degli scopi del trattamento, sia a quello del trattamento in sé, implementare delle appropriate misure tecniche e organizzative e delle procedure in una modalità tale da far sì che vi sia conformità al Regolamento e che si garantisca la protezione dei diritti dell'interessato[39]. Il secondo comma riguarda la protezione by default, ossia per impostazione predefinita, statuendo che il titolare dovrà implementare dei meccanismi che automaticamente garantiscano che siano trattati solo i dati personali necessari per ogni specifico scopo e in particolare che non siano

---

[36] Cfr. Considerando 61, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals: *"The protection of the rights and freedoms of data subjects with regard to the processing of personal data require that appropriate technical and organizational measures are taken, both at the time of the design of the processing and at the time of the processing itself, to ensure that the requirements of this Regulation are met. In order to ensure and demonstrate compliance with this Regulation, the controller should adopt internal policies and implement appropriate measures, which meet in particular the principles of data protection by design and data protection by default".*

[37] Cfr. Considerando 130, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission for: specifying standard forms in relation to the processing of personal data of a child; standard procedures and forms for exercising the rights of data subjects; standard forms for the information to the data subject; standard forms and procedures in relation to the right of access; the right to data portability; standard forms in relation to the responsibility of the controller to data protection by design and by default and to the documentation".*

[38] Cfr. Art. 22, co. 1, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation".*

[39] Cfr. Art. 23, co. 1, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject".*

raccolti e conservati i dati oltre minimo essenziale allo scopo, sia in termini di quantità che di tempo; nello specifico questi meccanismi dovranno assicurare che le informazioni non siano accessibili ad un indefinito numero di individui[40].

La Commissione Europea procede proponendo l'aumento dei propri poteri per poter adottare degli atti delegati che specifichino i criteri e le richieste dei due commi precedenti, e che, soprattutto per la protezione dei dati by design, siano applicabili ai vari settori, prodotti e servizi[41]. Inoltre, l'organo esecutivo dell'UE, si specifica, potrebbe dettare degli standard tecnici per i requisiti dei primi commi, attraverso una procedura di esame indicata in un articolo successivo della stessa proposta[42].

La codificazione dei due concetti di pbd e privacy by default assegna loro il ruolo di imperativo punto di riferimento in materia di privacy, pur essendo di per sé due lati della stessa medaglia[43]. La pbd, infatti, è rivolta verso l'interno, ossia opera nella fase di implementazione svolta dal titolare e il secondo concetto, invece, volge all'esterno, verso il fornitore del servizio, che deve somministrare all'utente un prodotto che per impostazione predefinita garantisca il massimo livello di tutela[44].

La seconda sezione della proposta del 2012 si occupa della sicurezza dei dati e al terzo comma dell'articolo 30 si indica un ulteriore potere della Commissione Europea, ossia la definizione di ciò che si intende per stato dell'arte in uno specifico settore e in particolari situazioni di trattamento, tenendo conto del progresso delle tecnologie e delle soluzioni per l'approccio pbd e di default[45]. Si può allora affermare che la protezione by design con la

---

[40] Cfr. Art. 23, co. 2, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals: "*2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals*".

[41] Cfr. Art. 23, co. 3, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services".*

[42] Cfr. Art. 23, co. 4, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)".*

[43] PASCUZZI (a cura di), *Il diritto dell'era digitale,* cit., 53.

[44] *Ibidem,* 53.

[45] Cfr. Art. 30, co. 3, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*:* "3. *The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organizational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in*

proposta sarebbe veicolata attraverso i criteri offerti dall'organo esecutivo dell'Unione, che poi sarebbero stati applicati dai singoli titolari del trattamento, ponendo attenzione alle specificità della situazione concreta.

Nel documento è interessante constatare che tra i compiti del responsabile del trattamento vi è anche il monitoraggio dell'implementazione e dell'applicazione del Regolamento con esplicito riferimento all'adozione della pbd[46]. Questa previsione genera una sorta di corresponsabilità tra il titolare e il responsabile e aumenta il controllo sull'adozione dell'approccio.

Infine, non si dimentica l'aspetto sanzionatorio, perché è vero che la pbd è stata inserita nella proposta, ma senza una norma che preveda una sanzione in caso di inottemperanza, la disciplina sarebbe imperfetta e la sua giuridicità contestabile. All'articolo 79 si statuisce dunque che ogni autorità preposta al controllo del trattamento dei dati dovrà avere il potere di infliggere delle sanzioni amministrative, le quali siano per il caso concreto effettive, proporzionate e dissuasive; nello specifico l'ammontare della somma dovuta dovrà essere fissato con riguardo alla natura, alla gravità e alla durata dell'infrazione e ad altri fattori, tra i quali le misure tecniche, organizzative e procedurali implementate in forza dell'articolo 23[47]. In breve, la mancata adozione di ciò che comporta l'approccio pbd è una violazione dell'articolo 23 e in quando tale può essere condannata da parte delle autorità degli stati membri con l'applicazione di una sanzione amministrativa. La cornice della sanzione per chi con intenzione o negligenza non adotta le politiche interne o non implementa le misure appropriate per assicurare e dimostrare la conformità con gli articoli 22, 23 e 30 è fissata con un massimo di un milione di euro o del 2 per cento del fatturato annuo di un'impresa commerciale[48].

---

specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies".

[46] Cfr. Art. 37, co. 1, let c), Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation".*

[47] Cfr. Art. 79, co. 1, Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. 2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach".*

[48] Cfr. Art. 79, co. 6, let. e), Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals*: "6. The supervisory authority shall impose a fine up to 1.000.000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently: (e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30".*

La proposta del 2012 richiede, quindi, che il titolare del trattamento adotti un approccio di privacy by design, ma non prescrive particolari metodi o livelli[49].

La successiva versione del testo compiuta dal Parlamento Europeo, invece, prevede dei requisiti più completi, descrive più nel dettaglio le metodologie che devono essere adottate, offre delle linee guida precise e tiene conto di aspetti molto più pratici. Per l'appunto, s'inseriscono tra le considerazioni iniziali dell'articolo sulla pbd, oltre allo stato dell'arte e dei costi dell'implementazione, l'attuale conoscenza tecnica, le best practices internazionali e il rischio rappresentato dal trattamento dei dati[50]. Non si innova solo in questo: il testo del Parlamento richiede che sia il titolare sia il responsabile del trattamento siano tenuti all'implementazione delle misure e che, in aggiunta, essi considerino tutto l'intero ciclo di gestione del dato, dalla raccolta, al trattamento e infine alla sua cancellazione[51]. I detentori dei dati dovrebbero concentrarsi in modo sistematico sulle garanzie procedurali, in modo che queste siano onnicomprensive e riguardino la precisione, la riservatezza, l'integrità, la sicurezza fisica e l'eliminazione del dato personale[52]. Tutto ciò comporta inevitabilmente l'assunzione di costi più o meno elevati per le società e fa sì che la progettazione tecnologica dei sistemi sia essenziale. Qualcuno si è chiesto allora se i costi interferiranno con la responsabilità del titolare e per quale motivo non ci sia alcun riferimento nelle norme alle figure fondamentali dei designers dei prodotti[53]. A queste domande non è facile fornire una risposta, ma si può notare che le autorità europee hanno cercato un compromesso tra gli interessi in gioco nella redazione definitiva del GDPR.

---

[49] GILBERT, *Proposed EU data protection regulation cit.*, 2: "*Article 23 of the Proposed Regulation would require the data controller, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical, physical, and organizational measures and procedures to ensure that the processing will meet the requirements of the Regulation and the rights of the data subject will be protected. Entities are expected to take into account the state of the art in application design, and the cost of implementation. No particular methods or steps are prescribed".*

[50] *Ibidem,* 4: "*The EU Parliament Version contains more comprehensive requirements. First, the criteria for the proper methodologies for the process of data protection by design would be significantly expanded and refined. These would include, in addition to looking at the state of the art already mentioned in the original draft, taking into account the current technical knowledge, international best practices, and the risks represented by the data processing".*

[51] *Ibidem,* 4: "*Further, the EU Parliament Version would require that both the controller and the processor, if any, implement appropriate and proportionate technical and organizational measures and procedures at the time of the determination of the purposes and means for processing and at the time of the processing itself. In addition, the EU Parliament Version would require that data protection by design processes and methodologies take into account the entire lifecycle management of personal data from collection to processing, and to deletion".*

[52] *Ibidem,* 4: *"It would require that data holders systematically focus on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security, and deletion of personal data. In addition, it would require that the result of any data protection impact assessment be taken into account when developing those measures and procedures".*

[53] COSTA, POULLET, *Privacy and the Regulation of 2012*, cit., 260: "*How will the cost of implementation interfere with the responsibility of the controller? Given that the design of technology is essential in this approach why is there no reference to designers?".*

Non resta dunque che analizzare il passaggio più importante del principio in oggetto nel quadro normativo europeo attuale, ossia il suo inserimento nel testo definito del GDPR. La protezione dei dati personali fin dalla progettazione è qui indicata come uno dei principi in materia di trattamento dei dati personali. Il rango di principio non può che essere un riconoscimento molto rilevante e a dichiararlo non è più soltanto una riflessione dottrinale, o un'agenzia indipendente, ma è una norma giuridica vincolante per tutti gli Stati Membri dell'Unione Europea.

2. L'art. 25 del GDPR

Prima di procedere con l'analisi dell'articolo 25 è necessario riferirsi ad affermazioni contenute nella parte iniziale del GDPR. Nel Regolamento oggetto d'analisi, al considerando numero 78, si richiede al titolare del trattamento di adottare delle politiche interne e delle misure che soddisfino i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita. Si offrono tra l'altro degli esempi concreti di possibili misure implementabili: la riduzione del minimo dell'utilizzo dei dati, la pseudonimizzazione, una maggiore trasparenza sulle funzioni e sullo stesso trattamento, la partecipazione dell'interessato nel controllo dei dati e la possibilità per il titolare di creare e migliorare le caratteristiche della sicurezza[54]. È interessante sottolineare che nello stesso paragrafo si manifesta l'esigenza di incoraggiare i produttori dei prodotti, dei servizi e delle applicazioni, per il cui funzionamento si pone in essere un trattamento di dati personali, a tenere conto del diritto alla loro protezione nelle fasi di sviluppo, di progettazione, di selezione e di utilizzo di questi strumenti, vagliando lo stato dell'arte e così permettendo ai titolari e ai responsabili di adempiere agli obblighi prescritti[55]. Si aggiunge che il principio di pbd e by default, dovrebbero essere considerati anche per un appalto pubblico, il che significa che non solo i privati sono coinvolti, ma anche gli enti statali, aspetto non di poco conto.

Al capo quarto del GDPR, in materia di obblighi generali del titolare e del responsabile del trattamento, si trova finalmente l'articolo 25, rubricato *"Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"*:

[54] Cfr. Considerando 78, Reg. 27 aprile 2016, n. 2016/679.

[55] *Ibidem: "In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici"*.

"*1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.*

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo"[56].

Il titolare del trattamento deve mettere in atto le misure tecniche e organizzative adeguate per assicurare una protezione dei dati personali fin dalla progettazione.

Ora, operando un confronto tra questa norma e il testo dell'articolo 23 della proposta della Commissione, è chiaro che siano stati compiuti dei cambiamenti nel corso dell'elaborazione del definitivo articolo 25. In primo luogo, se nel 2012 erano stati forniti solo i criteri dello stato dell'arte e dei costi, qui si hanno molti più elementi da considerare: la natura dell'ambito di applicazione, del contesto e delle finalità del trattamento dei dati, e i rischi insiti nel trattamento per i diritti e le libertà delle persone fisiche, i quali hanno delle probabilità e gravità diverse tra di loro. L'aspetto temporale, però, rimane invariato, la privacy by design attraverso le sue misure dovrà essere adottata sia ex ante, sia a trattamento pendente. Secondariamente, le adeguate misure organizzative e procedurali del GDPR, di cui si fornisce l'esempio della pseudonimizzazione, hanno dei fini ulteriori rispetto a ciò che era indicato nel testo della Commissione: esse non sono volte soltanto a garantire la conformità

[56] Si è scelto di riportare integralmente l'articolo 25 vista la sua centralità nell'attuale discussione, prendendo a riferimento per praticità la sua versione italiana ricavabile dal sito europeo <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679>.

del trattamento alla normativa, ma anche ad attuare efficacemente gli altri principi fondamentali di protezione dei dati, come la minimizzazione, e a tutelare generalmente i diritti degli interessati.

Per quanto riguarda il secondo comma che disciplina la protezione per impostazione predefinita, l'articolo 25 innova il testo precedente quando indica che l'obbligo vale per la quantità delle informazioni raccolte, per il periodo di tempo e altresì per la portata del trattamento e l'accessibilità dei dati; poi si specifica che il fatto di non essere un dato accessibile ad un numero indefinito di persone è legato al necessario intervento di una persona fisica per la sua conoscibilità.

Inoltre, rispetto alla proposta si perdono completamente i due commi 3 e 4 dell'articolo 23 che accordavano maggiori poteri alla Commissione per atti delegati chiarificatori e per la fissazione di standard. La regolamentazione di secondo livello sarebbe stata utile per una maggiore precisazione di contenuto per i titolari, su un piano meno vincolante e più capace di adattarsi all'evoluzione della tecnologia[57]. Allo stesso tempo, però, la scelta evita che gli standard compromettano la neutralità tecnologica delle disposizioni, a vantaggio di una migliore capacità adattiva, di una maggiore flessibilità e di una possibile competitività nelle soluzioni auto-imposte dagli operatori[58].

Oggi, residua soltanto un terzo comma che fa riferimento ai meccanismi di certificazione di cui presto si dirà e di cui si tratterà con ampio respiro nel quarto capitolo della presente tesi. Questo meccanismo certificatorio potrà essere uno strumento atto a dimostrare la conformità del trattamento ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita. Il passaggio tra le due versioni tiene conto della realizzazione concreta di criteri e strumenti che possano essere davvero utili per le imprese: sarebbe stato più difficile probabilmente prestare adeguata attenzione ai lavori della Commissione Europea, mentre è sembrato più immediato creare la possibilità di rivolgersi ad enti certificatori esterni per vedersi garantita la compatibilità delle proprie misure con il GDPR e così diminuire il rischio di essere dichiarati responsabili per l'inosservanza degli obblighi di cui all'articolo 25.

A parere di chi scrive, il testo definitivo ha il pregio di indicare una serie di considerazioni che il titolare del trattamento dovrebbe avere ben presenti una volta che si accinge a definire le misure adottabili nel suo caso concreto; allo stesso tempo è molto aperto e di non fornisce molti esempi di pratiche utilmente implementabili, lasciando alla discrezione del titolare e del suo informatico. Non si deve dimenticare però che la scelta di non elencare le tecnologie e le procedure di riferimento è coerente con una tecnica legislativa tecnologicamente neutrale: la norma fissa i principi e le varie linee guida, e sta

[57] A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, in *Contr. impr. Europa,* 2015, fasc. 1, 215.
[58] *Ibidem,* 215.

al progresso della scienza fornire soluzioni sempre più nuove ed adeguate allo scopo. Il titolare può pescare le misure in un mare pieno di pesci dalle molte varietà, in base a ciò che più si confà al suo gusto e alla sua sensibilità, sapendo che più il pesce è grande e ricco di buona carne, più sarà consapevole di aver scelto bene. Insomma, si apre alle più varie misure tecniche e organizzative, sempreché siano adeguate ed efficaci. Si ricorda che nel Considerando numero 78 in realtà vengono fornite delle esemplificazioni, come si è sopra riportato e che queste possono essere dei punti di partenza per i titolari del trattamento. In più, si auspica che si consolidi un'interpretazione dell'articolo 25 nei lavori delle Autorità di controllo e quindi del nostro Garante per la Protezione dei Dati personali. Poi, passato un iniziale periodo di transizione, le stesse corti europee saranno chiamate a stabilire quali siano nel dettaglio le misure che applicano correttamente i nuovi principi fondamentali del quadro normativo europeo.

Si ritiene che lo strumento della certificazione possa essere offrire un salto di qualità per le società: la privacy by design potrebbe essere un elemento di sicurezza e di incentivo per i soggetti commerciali, come si dirà successivamente e come dimostrano già ad oggi delle esperienze estere. Ovviamente, i costi della privacy per le imprese potrebbero aumentare di non poco; si può pensare che sarà la futura giurisprudenza europea a dover affrontare il problema dell'approccio pbd in relazione ai suoi costi, perché un investimento elevato può essere sintomo di maggior attenzione, ma non è un fattore così certo. Ciò che è certo è che si dovranno fare i conti con l'applicazione del GDPR, a partire dal 25 maggio del 2018.

Si potrebbe ora evidenziare un difetto nell'articolo 25: la norma fa riferimento ai titolari del trattamento, lasciando fuori chi in concreto opera sulla progettazione, ossia i programmatori, i produttori e gli sviluppatori[59]. Ciò potrebbe essere mitigato dal fatto che si prevedono delle accortezze che di default garantiscono la protezione dei dati personali, che si ha l'incentivo per il titolare ad avere dei sistemi informatici conformati alla pbd, quantomeno per non essere ritenuto responsabile, e che nel GDPR si ha una visione della materia concentrata sulla gestione dell'informazione. Appunto, la disciplina della privacy by design sembra focalizzarsi su una corretta e sicura gestione dei dati da parte di chi li detiene[60].

Se è evidente che l'articolo 25 ricopre un ruolo centrale per l'oggetto di discussione, è solo proseguendo l'analisi del GDPR che è possibile fornire un quadro completo della nuova protezione dei dati fin dalla progettazione. La

[59] Anche se c'è chi ha commentato, già a partire dalla proposta di Regolamento, che l'articolo di riflesso si rivolge anche ai produttori di sistemi IT. Si veda B. J. KOOPS, R. LEENES, *Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*, 28 *Int. Rev. Law Comput. Tech.* 1 (2013).
[60] *Ibidem,* 217.

sicurezza, si affermava nel primo capitolo, viaggia di pari passo con la privacy. Questa affermazione è da considerarsi valida anche per il Regolamento del 2016.

All'articolo 30 si richiede al titolare del trattamento e all'eventuale responsabile di tenere un registro delle attività svolte, il quale deve contenere una serie di informazioni, tra le quali, ove possibile, la descrizione generale delle misure di sicurezza tecniche e organizzative assunte ai sensi dell'articolo 32 comma 1[61]. Per l'appunto quest'ultima norma riprende le parole iniziali utilizzate nell'articolo 25 e obbliga il titolare e il responsabile a mettere in atto quelle adeguate misure tecniche e organizzative che già si prescrivono, affinché si garantisca un livello di sicurezza adatto al rischio. Si elencano all'uopo una serie di misure: "*la pseudonimizzazione, la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*"[62]. Se nell'articolo sulla protezione dei dati fin dalla progettazione non si elencano delle esemplificazioni e, come si è detto, ciò potrebbe essere un vantaggio per l'interpretazione della norma, qui si opera una scelta diversa. Si potrebbe ritenere che, viste soprattutto le parole comuni, i due articoli debbano essere letti congiuntamente: il titolare mette in atto le misure per rispettare il principio di pbd e allo stesso tempo garantire la sicurezza del trattamento. In entrambe le norme emerge apertamente l'importanza della valutazione del rischio, che in relazione alla sicurezza dovrà vagliare la possibilità di distruzione, di perdita, di modifica, di divulgazione non

[61] Cfr. Art. 30, co. 1, Reg. 2016/679*: "1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: […] g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1".* È necessario specificare qui che ai sensi del quinto comma dell'articolo 30 dall'obbligo di tenere il registro sono esenti le imprese o le organizzazioni con meno di 250 dipendenti, a meno che non vi sia la possibilità di un rischio per i diritti e per le libertà dell'interessato, o che il trattamento non sia occasionale o che includa delle categorie particolari di dati (di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10).

[62] Cfr. Art. 32, co.1, Reg. 2016/679: *"1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".*

autorizzata o di accesso, in modo accidentale o illegale, in relazione ai dati personali trasmessi, conservati o comunque trattati[63].

Poi, anche nell'articolo 32 si statuisce che l'adesione ad un meccanismo di certificazione potrebbe essere utilizzata per dimostrare la conformità con il GDPR. In aggiunta, si prevede la stessa possibilità appena citata anche per l'adozione di un codice di condotta approvato ai sensi dell'articolo 40[64].

La presenza di questi codici è volta a contribuire alla corretta applicazione del GDPR ed è compito degli Stati Membri, delle autorità di controllo, del comitato previsto all'interno del Regolamento e della Commissione incoraggiarne l'elaborazione, con l'attenzione nei confronti delle specificità dei settori del trattamento e delle esigenze delle varie tipologie di imprese[65]. I soggetti che possono elaborare i codici di condotta, modificarli o prorogarli sono le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento, al fine di precisare cosa significhi in termini concreti applicare le nuove norme[66]. Al secondo comma dell'articolo appena citato vengono elencati a titolo di esempio una serie di norme del GDPR che potrebbero essere meglio esplicate grazie all'adozione dei codici di condotta e tra queste sono comprese le misure e le procedure di cui agli articoli 24, 25, 32, che come si è visto, contengono la disciplina della privacy by design e by default[67].

I codici di condotta, e le loro successive modifiche o proroghe, sono elaborati dalle associazioni e dagli altri organismi, ma devono essere vagliati dalle autorità di controllo, attraverso un parere di conformità al Regolamento e, se approvati, sono da queste registrati e pubblicati[68].

---

[63] Cfr. Art. 32, co. 2, Reg. 2016/679: *"2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".*

[64] Cfr. Art. 32, co. 3, Reg. 2016/679: *"3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo".*

[65] Cfr. Art. 40, co. 1, Reg. 2016/679: *"1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese".*

[66] Cfr. Art. 40, co. 2 Reg. 2016/679: "*2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento […]".*

[67] Cfr. Art. 40, co. 2, lett. h), Reg. 2016/679: *"h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32".*

[68] Cfr. Art. 40, co. 5, Reg. 2016/679: *"L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate. 6. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice".*

Il GDPR inserisce non solo i codici come strumenti per garantirne l'adeguata implementazione, ma anche la certificazione. Ai sensi dell'articolo 42 infatti si incoraggia, particolarmente a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati, di sigilli e di marchi[69]. La certificazione è volontaria, non riduce la responsabilità dei soggetti ed è rilasciata da organismi accreditati presso le autorità di controllo o l'organismo nazionale di accreditamento. Come si vedrà nel quarto capitolo non mancano all'estero delle esperienze certificatorie già in atto.

Se tutto questo apparato di garanzie non fosse sufficiente e il trattamento dei dati non fosse conforme, le autorità di controllo infliggeranno delle sanzioni ammnistrative pecuniarie, come previsto dall'articolo 83 del GDPR. Quando un'autorità deve agire in questo senso, sia nel momento della decisione sull'imposizione, sia in quello della fissazione dell'ammontare della somma dovuta, essa dovrà tenere in debito conto vari criteri, tra i quali il grado di responsabilità del titolare del trattamento o del responsabile con riferimento alle misure tecniche e organizzative degli articoli 25 e 32[70]. Gli obblighi contenuti in queste norme se non assolti possono condurre all'imposizione di sanzioni amministrative pecuniarie fino a dieci milioni di euro o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore[71].

Ciò che si può dunque affermare è che per il GDPR la privacy by design è un obbligo vero e proprio, che è soggetto alla valutazione della probabilità dei rischi per le violazioni dei diritti e delle libertà. Le aziende, come si è ripetuto più volte, devono cercare di adottare delle misure già quando progettano le modalità e le politiche del trattamento dei dati che raccolgono, operando una valutazione del rischio che le attività comportano per gli utenti. Questa valutazione è un aspetto caratteristico del Regolamento del 2016, visto che si prevede all'articolo 35 il Privacy Impact Assessment*:* quando il trattamento prevede l'uso di nuove tecnologie, considerati la sua natura, l'oggetto, il contesto e la finalità, e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, si dovrà effettuare una valutazione di impatto sulla

[69] Cfr. Art. 42, co. 1, Reg. 2016/679: *"Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese".*

[70] Cfr. Art. 83, co. 2, let. d), Reg. 2016/679: *"d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32".*

[71] Cfr. Art. 83, co. 4, Reg. 2016/679: *"4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43".*

protezione dei dati[72]. Si tratta di un meccanismo erede di quel documento programmatico sulla sicurezza che si è presentato nel primo capitolo di questa tesi.

La soluzione di pbd sarà ricercata nel caso concreto: ogni categoria di trattamento, ogni singolo trattamento, sarà circondato da limiti e garanzie suoi propri e collegati al rischio percepito, ma saranno tutti presenti fin dalla sua progettazione. Il tempo e la tecnologia sono due variabili sempre in movimento e giocheranno sempre un ruolo di punta per i titolari del trattamento dei dati personali, i quali sono delegati ad attuare le soluzioni per il caso concreto.

A livello giuridico la normativa sarà più flessibile, non rischierà di diventare obsoleta a causa del costante progresso tecnologico, i dati personali saranno protetti con maggiore sicurezza ed efficacia, perché si avrà una protezione ex ante più adeguata e funzionale. È vero anche che i costi sono molto alti per le aziende e che sarà più difficile dimostrare la presenza di responsabilità perché la prova richiede alle autorità delle valutazioni molto più complesse, con il rischio che siano in qualche modo discrezionali e non certe, dovendosi considerare l'organizzazione e l'allocazione delle risorse per la protezione della privacy, per cui le piccole e le grandi imprese potrebbero soggiacere ad un trattamento differente.

Allo stesso tempo la privacy assume grazie al GDPR un ruolo ancora più significativo e un'importanza vitale per i soggetti economici; infatti non c'è più la possibilità di eludere in qualche modo il sistema predisponendo semplicemente dei regolamenti interni all'azienda pieni zeppi di scappatoie perché le misure rispettose della pbd e privacy by default sono vincolanti a meno che non si voglia subire un pesante aggravio sanzionatorio.

In conclusione, si possono riportare alcune delle parole del discorso di Viviane Reding, che è un membro della Commissione Europea responsabile per *l'information society* e i media, tenutosi a Bruxelles di fronte al Parlamento Europeo nell'occasione del *Data Protection Day,* il 28 gennaio del 2010:

> "*Here we need a change of approach: Businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle. Privacy by Design is a principle that is in the interest of both citizens and businesses. Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn have a positive*

[72] Cfr. Art. 35, co. 1, Reg. 2016/679: *"1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".*

impact on the economy. I have seen some encouraging examples, but much more needs to be done"[73].

La pbd rappresenta un cambiamento di approccio, lo si è ampiamente dimostrato; è un principio che avvantaggia gli individui e allo stesso tempo potrebbe creare dei benefici ai soggetti commerciali. Si è detto come sia stato esplicitato solo mercé della nuova normativa europea in materia di protezione dei dati; eppure, analizzando la legislazione precedente, sia italiana, sia sovranazionale, tanto cogente, quanto di soft law, potrebbero essere rilevate delle sue tracce precedenti, che ne dimostrano la bontà e la non così totale novità.

3. Alla ricerca della privacy by design nella normativa italiana ed europea e nei documenti di soft law

È certamente vero che la privacy by design ha trovato la sua finale codificazione nel GDPR; compiendo un'analisi storica e interpretativa, si possono, però, rilevare delle tracce di questo principio già in precedenti norme europee ed italiane e in documentazioni di soft law provenienti dalle autorità garanti della privacy o dalla Commissione Europea. In questo paragrafo si intende riportare questo percorso, che si è rivelato un passo fondamentale per comprendere che il contenuto della stesura finale dell'articolo 25 del Regolamento 2016/579 si è formato sì grazie ai lavori redazionali degli organi europei, ma anche grazie alla presenza nel contesto di norme e di riflessioni nel corso degli ultimi anni.

Iniziando con la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (Data Protection Directive*)* si può rilevare che si fa riferimento alle misure tecniche ed organizzative che sono lo scheletro dell'attuale pbd. In particolare, l'articolo 17 potrebbe essere interpretato in via estensiva per includere nel quadro normativo le prescrizioni che implicitamente conducono alla privacy by design*,* perché volte a prevenire un illecito trattamento[74]. Appunto, il testo non contiene un esplicito obbligo, ma in via indiretta conduce allo stesso risultato di

[73] Il discorso è ricavabile al sito: <http://europa.eu/rapid/press-release_SPEECH-10-16_it.htm>.
[74] Cfr. Art. 17, co. 1, Dir. 95/46/CE*: "1. Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere"*.

implementazione[75]. Tra l'altro, si può ritrovare un accenno in tal senso nel considerando numero 46 della stessa direttiva, nel quale si afferma che la tutela dei diritti e delle libertà delle persone richiede l'adozione di adeguate misure tecniche ed organizzative, da attuare nel momento della progettazione e in quello dell'esecuzione del trattamento, con lo scopo di garantire la sicurezza dei dati ed impedire ogni trattamento non autorizzato[76]. L'accenno alla progettazione dimostra che all'epoca era già presente una sensibilità tale da considerare la necessità di misure ex ante per la protezione dei dati personali.

La successiva Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al "trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche" è più esplicitamente ricollegabile alla pbd[77]. All'articolo 14 relativo alle caratteristiche tecniche ed alla standardizzazione si prevede, infatti, che le misure richieste debbano essere adottate per assicurare che l'attrezzatura sia costruita in un modo che sia compatibile con il diritto dell'utilizzatore di proteggere e controllare l'uso dei suoi dati personali[78]. Insomma, anche qui sono state poste le prime premesse per la pbd: come si legge nel considerando numero 30 di questa direttiva, i sistemi per la fornitura di reti e di servizi di comunicazione elettronica dovrebbero essere progettati per limitare al minimo la quantità di dati personali necessari[79].

In nuce, le norme citate contengono delle promozioni indirette all'approccio di pbd, anche se in concreto non sono state sufficienti ad assicurare che la privacy fosse incorporata nelle tecnologie ICT[80].

---

[75] Si veda l'Opinion of the European Data Protection Supervisor on promoting trust in the Information Society by fostering data protection and privacy del 18.3.2010, 7: *"The current data protection Directive does not contain an explicit requirement for PbD. However, it includes provisions which indirectly, in different situations, may well demand the implementation of the principle of PbD. In particular, Article 17 requires that data controllers implement appropriate technical and organization measures to prevent unlawful data processing".*

[76] Cfr. Considerando 46, Dir. 95/46/CE.

[77] *Ibidem,* 7: "*The ePrivacy Directive is more explicit. Article 14.3 provides that "Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications)". However, this provision has never been used"*.

[78] Cfr. Art. 14, co. 3, Dir. 2002/58/CE*: "3. Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardisation in the field of information technology and communications"*.

[79] Cfr. Considerando 30, Dir. 2002/58/CE.

[80] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society, 7: *"Whereas the above provisions of the two Directives are helpful towards the promotion of privacy by design, in practice they have not been sufficient in ensuring that privacy is embedded in ICT"*.

Una prima riflessione sulla necessità di inserire la privacy by design in modo esplicito in un nuovo quadro normativo europeo è giunta nel 2009 dal Gruppo Articolo 29[81]. Nel documento intitolato *"The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data",* si legge che gli utenti dei servizi ICT, che sono sia gli individui, che i soggetti commerciali e il settore pubblico stesso, non sono nella posizione di attuare da sé le misure di sicurezza atte a proteggere i propri dati; ciò premesso, i servizi e le tecnologie dovrebbero essere già progettati in modo da garantire la privacy[82]. Il Gruppo ex Art. 29 auspica a questo fine la redazione di un nuovo quadro normativo europeo che comprenda un *"broader and consistent principle of privacy by design",* che sia vincolante per i tecnici, i produttori e i titolari dei trattamenti dei dati, ampliando apprezzabilmente il cerchio dei soggetti coinvolti e obbligati nell'incorporazione delle regole e nella sua dimostrazione[83]. A parere dell'organismo europeo questo principio dovrebbe essere definito in una modalità tecnologicamente neutrale, affinché possa durare per un lungo periodo di tempo in un contesto di rapidi cambiamenti tecnologici e sociali[84]. Per minimizzare le difficoltà nel definire e specificare ciò che si intende in concreto per pbd l'autorità propone di sviluppare e considerare la stesura di standard tecnici, che possono essere sia generali che particolari[85]. Nel momento in cui il

[81] Il Gruppo è così chiamato perché è stato istituito dall'art. 29 della Data Protection Directive. Si tratta di un organismo consultivo e indipendente, il quale è composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal Garante Europeo della Protezione dei Dati e da un rappresentante della Commissione. Le informazioni sono ricavabili dal sito del nostro Garante Privacy: <http://www.garanteprivacy.it/home/attivita-e-documenti/attivita-comunitarie-e-internazionali/cooperazione-in-ambito-ue/gruppo-di-lavoro-ex-articolo-29>.

[82] Article 29 Data Protection Working Party, *"The Future of privacy, joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data",* WP 168 02356/09/EN, 13: *"Users of ICT services – business, public sector and certainly individuals – are not in a position to take relevant security measures by themselves in order to protect their own or other persons' personal data. Therefore, these services and technologies should be designed with privacy by default settings*".

[83] *Ibidem,* 13: *"It is for these reasons that the new legal framework has to include a provision translating the currently punctual requirements into a broader and consistent principle of privacy by design. This principle should be binding for technology designers and producers as well as for data controllers who have to decide on the acquisition and use of ICT. They should be obliged to take technological data protection into account already at the planning stage of information-technological procedures and systems. Providers of such systems or services as well as controllers should demonstrate that they have taken all measures required to comply with these requirements".*

[84] *Ibidem,* 14: "*Such principle should be defined in a technologically neutral way in order to last for a long period of time in a fast changing technological and social environment. It should also be flexible enough so that data controllers and DPAs will, on a case by case basis, be able to translate it in concrete measures for guaranteeing data protection".*

[85] *Ibidem,* 14: *"Technological standards should be developed and taken into consideration in the phase of system analysis by hardware and software engineers, so that difficulties in defining and specifying requirements deriving from the principle of 'privacy by design' are minimized.*

principio non risulti sufficiente a garantire la tutela e serva un approccio spendibile in una situazione reale si dovrebbero prevedere le misure specifiche per ogni contesto dotato della sua peculiarità, come ad esempio le tecnologie radio o i social networks[86].

Il documento del Gruppo Art. 29 ha riscosso molto successo in ambito europeo. Il Garante Europeo per la Protezione dei Dati (d'ora in poi anche GEPD) non è a questo punto rimasto inattivo e nel marzo del 2010 ha pubblicato un parere molto rilevante: *the Opinion on promoting trust in the Information Society by fostering data protection and privacy*[87].

Il documento citato si occupa della necessità di integrare la privacy dal principio del trattamento e dedica ampio spazio alla pbd, indicando due modalità di azione: per primo è necessario definire un principio generale e vincolante nel nuovo quadro normativo europeo e poi è auspicabile incorporarlo in particolari aree applicative dell'ICT, tra le quali ne vengono indicate tre, ossia la Radio Frequency Identification (RFID), le social network applications e le browsers applications[88].

L'aspetto più interessante del parere è che il GEPD ritiene che la privacy by design sia lo strumento chiave per generare una maggior fiducia nelle persone sulle tecnologie ICT, dal momento che il loro diritto risulta tutelato per tutto il ciclo di vita del prodotto o del servizio, dal primo passaggio di progettazione, alla sua ultima evoluzione, all'utilizzo e alla sua eliminazione. L'autorità spiega anche che questo principio implica e necessita l'adozione di varie azioni ulteriori, tra le quali la riduzione o l'eliminazione dei dati personali,

---

Such standards may be general or specific with regard to various processing purposes and technologies".

[86] *Ibidem,* 15: *"The privacy by design principle may not be sufficient to ensure, in all cases, that the appropriate technological data protection principles are properly included in ICT. There may be cases where a more concrete 'hands on approach' may be necessary. To facilitate the adoption of such measures, a new legal framework should include a provision enabling the adoption of specific regulations for a specific technological context which require embedding the privacy principles in such context. […] The above would facilitate the adoption, in specific cases, of specific legislative measures embedding the concept of 'privacy by design' and ensuring that adequate specifications are provided. For example, this may be the case with RFID technology, social networks, behavioral advertisement, etcetera".*

[87] Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society del 18.3.2010, in Rete: <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf.>

[88] Opinion of the European Data Protection Supervisor on promoting trust in the Information Society, 2: *"In order to compel compliance with this principle, the Opinion discusses the need to provide for the principle of "privacy by design" into the data protection legal framework in at least two different ways. First, by incorporating it as a general, binding principle and, second, by incorporating it in particular ICT areas, presenting specific data protection/privacy risks which may be mitigated through adequate technical architecture and design. These areas are Radio Frequency Identification (RFID), social network applications and browsers applications. Finally, the Opinion makes suggestions regarding other tools and principles aiming at protecting individual's privacy and data protection in the ICT sector*".

la prevenzione dai trattamenti non necessari o indesiderati, la fornitura di strumenti per accrescere il controllo degli individui sulle proprie informazioni, la vera e propria incorporazione delle misure nell'architettura dei sistemi ICT o nelle organizzazioni strutturali dei soggetti compiono i processi[89]. Con una frase iconica nel parere si afferma che "*when information and communication technologies are built according to the principle of PbD, the risks to privacy and data protection may be significantly minimized*"[90]*.* Lo scopo diretto della privacy by design è la diminuzione del rischio di violazioni della riservatezza e della protezione dei dati personali.

Il parere tra l'altro si mostra in linea con il documento del Gruppo Articolo 29 perché auspica l'inclusione del principio in questione nella normativa e nelle politiche dell'Unione Europea. Nel dettaglio, il GEPD raccomanda alla Commissione di seguire quattro linee di azione: proporre l'introduzione di una previsione generale di pbd nel quadro normativo per la protezione dei dati, elaborarla attraverso la predisposizione di disposizioni specifiche in differenti settori sulla base dell'articolo 17 della Dir. 95/45/CE (da cui si deduce l'importanza di aver citato la norma nella presente analisi), includere l'approccio in qualità di principio guida nell'Agenda Digitale Europea e infine inserire il principio anche in altre iniziative europee[91].

Un'ulteriore indicazione è la necessità che la privacy by design sia tecnologicamente neutrale: la norma generale non deve regolare la tecnologia, ma piuttosto ordinare l'integrazione delle regole esistenti in materia nei sistemi e nelle soluzioni, in modo che la portata del principio si possa interpretare in ogni caso specifico e che la conformità ad esso sia obbligatoria in ogni stadio[92].

---

[89] *Ibidem,* 4: *"PbD can entail different actions, depending on the particular case or application. For example, in some cases it may require eliminating/reducing personal data or preventing unnecessary and/or undesired processing. In other cases, PbD may entail offering tools to enhance individuals' control over their personal data. Such measures should be considered when standards and/or best practices are defined. They can also be incorporated into the architecture of information and communication systems, or in the structural organizations of the entities that process personal data".*

[90] *Ibidem,* 5.

[91] *Ibidem,* 8*: "In the light of the above, the EDPS recommends the Commission to follow four courses of action: Propose to include a general provision on PbD in the legal framework for data protection. Elaborate this general provision in specific provisions, when specific legal instruments in different sectors are proposed. These specific provisions could already now be included in legal instruments; on the basis of Article 17 of the Data Protection Directive (and other existing law). Include PbD as a guiding principle in Europe's Digital Agenda. Introduce PbD as a principle in other EU-initiatives (mainly non legislative)*.

[92] *Ibidem,* 9: *"First and most important, a general privacy by design principle should be technologically neutral. The principle should not intend to regulate technology, i.e. it should not prescribe specific technical solutions. Instead, it should mandate that existing privacy and data protection principles be integrated into information and communication systems and solutions. This would allow stakeholders, manufacturers, data controllers and DPAs, to interpret the meaning of the principle in each individual case. Second, compliance with the principle should be mandatory at different stages, from the creation of standards and the design of the architecture to their implementation by the data controller"*.

Le particolarità dei vari settori tecnologici fanno sì che lo sviluppo del principio sia strettamente legato al suo contesto applicativo; così spesso si dovrà includere un riferimento esplicito alla nozione di pbd nelle norme valide in quel singolo ambito. Se si prevede un piano di azione per un'area specifica, i soggetti coinvolti dovranno sistematicamente assicurare l'applicazione del quadro normativo e in più garantire che la tecnologia sia sviluppata con la privacy by design bene in mente[93].

Questo documento del Garante Europeo è stato di fondamentale aiuto per i lavori della Commissione Europea in relazione alla proposta di regolamento del 2012, testo che introduce esplicitamente la pbd in un progetto normativo dell'Unione sulla protezione dei dati personali[94].

In realtà, il principio in oggetto non segue solo la strada dell'elaborazione del GDPR, di cui si è già dato conto nei precedenti paragrafi, ma si inserisce altresì nella storia di altri settori dell'ordinamento europeo. A partire dal 2012, infatti, la pbd è stata inserita in tre regolamenti e due decisioni.

In primo luogo, si può ritrovare un riferimento nel Regolamento n. 1024/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012 relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno (detto anche Regolamento IMI), il quale disciplina un sistema informatico online multilingue che consente lo scambio informativo tra le pubbliche amministrazioni dell'Unione, per migliorarne le comunicazioni, l'accessibilità e la flessibilità[95]. Al considerando numero 7 si fa presente che l'IMI è stato sviluppato considerando da subito la privacy by design e rispettando le disposizioni in materia di protezione dei dati, per offrire un livello di sicurezza molto elevato, maggiore a quello della posta ordinaria, del telefono,

---

[93] *Ibidem,* 10: *"How exactly the PbD principle will be developed will depend on each particular sector and situation. For example, when Commission initiatives are accompanied by legislative proposals on a specific ICT sector, in many cases it will be appropriate to include an explicit reference to the notion of PbD applicable to the design of the particular ICT application/system. If action plans for a specific area are designed, they should systematically ensure the application of the legal framework and more specifically guarantee that the relevant ICT technology is built with privacy by design in mind*".

[94] Peraltro il GEPD ha inserito nella Decisione 17 dicembre 2012 n. 504 sull'adozione del suo regolamento interno, all'articolo 38 la seguente disposizione: *"1. Ai sensi dell'articolo 46, lettera e), del regolamento, il GEPD segue l'evoluzione delle tecnologie dell'informazione e della comunicazione. Nell'esercizio di tale funzione, il GEPD intende individuare le tendenze emergenti con un potenziale impatto sulla protezione dei dati, stabilendo contatti con le parti interessate, svolgendo attività di sensibilizzazione su possibili aspetti della protezione dei dati e fornendo consulenza sul modo di integrare le preoccupazioni in materia di protezione dei dati in progetti pertinenti, promuovendo i principi della tutela della vita privata fin dalla progettazione («privacy by design») e della tutela della vita privata per impostazione predefinita («privacy by default») e, se necessario, adattando le metodologie di controllo all'evoluzione tecnologica".* Il principio perciò sarà promosso dal Garante nelle sue attività di sensibilizzazione e di consulenza, il che può voler dire che aumenterà la conoscenza e la condivisione delle realtà europee sul tema.

[95] Le informazioni sono ricavabili dal sito: <ec.europa.eu/imi-net>.

del fax o della posta elettronica[96]. In questo contesto la pbd è un principio applicato per proteggere al meglio i dati trattati dalle amministrazioni e ha condotto ad un sistema informatico efficiente e ampiamente utilizzato.

Un altro ambito concreto in cui si è impiegato il principio è la piattaforma online per la risoluzione delle controversie in via extragiudiziale, disposta per chi risiede nell'Unione Europea e ha riscontrato un problema con un acquisto di un prodotto o un servizio via Internet, venduti da un commerciante che ha sede sempre nell'UE, ovvero per chi è un commerciante con sede nell'UE ed ha una lite con un suo cliente/consumatore[97]. La piattaforma, definita ODR, è stata istituita dal Regolamento del Parlamento Europeo e del Consiglio del 21 maggio 2013 n. 524 relativo alla risoluzione delle controversie online dei consumatori e risulta essere uno strumento che consente una tutela più veloce, più semplice e sicuramente meno costosa rispetto a quella giudiziale, dal momento che è un sito web facilmente accessibile e soprattutto gratuito, operativo in tutte le lingue ufficiali dell'Unione. L'articolo 5 del presente Regolamento 2013/524 dispone che lo sviluppo della piattaforma ODR e il suo funzionamento e la manutenzione assicurano, per quanto sia possibile, la tutela della vita privata fin dalla progettazione[98]. Anche qui il principio ha contribuito alla predisposizione di uno strumento efficiente e utile per i cittadini europei.

Successivamente, ma sicuramente di minor impatto, si ritrova la pbd nella Decisione del Consiglio del 3 dicembre 2013 n. 743 che stabilisce il programma specifico di attuazione del programma quadro di finanziamento dei progetti di ricerca e di innovazione per gli anni dal 2014 al 2020, il cosiddetto Orizzonte

---

[96] Cfr. Considerando 7, Regolamento (UE) n. 1024/2012 del Parlamento europeo e del Consiglio del 25 ottobre 2012, relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno e che abroga la decisione 2008/49/CE della Commissione («regolamento IMI») G.U. L. 316 del 14 novembre 2012: *"In base al principio della «privacy by design» (tutela della vita privata fin dalla progettazione), l'IMI è stato sviluppato fin dall'inizio considerando e rispettando le disposizioni della normativa in materia di protezione dei dati, in particolare tenendo conto delle restrizioni imposte riguardo all'accesso ai dati personali scambiati nell'IMI. L'IMI offre pertanto un livello di protezione e di sicurezza molto più elevato rispetto ad altri mezzi per lo scambio di informazioni come la posta ordinaria, il telefono, il fax o la posta elettronica".*

[97] Il sito nel quale è possibile fare reclamo per un prodotto o servizio acquistato online è: <https://webgate.ec.europa.eu/odr/main/?event=main.home.show>.

[98] Cfr. Art. 5, co. 1, Regolamento (Ue) del Parlamento Europeo e del Consiglio del 21 maggio 2013 N. 524 relativo alla risoluzione delle controversie online dei consumatori e che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (regolamento sull'ODR per i consumatori): *"1. La Commissione sviluppa la piattaforma ODR ed è responsabile per quanto riguarda il suo funzionamento, comprese tutte le funzioni di traduzione necessarie ai fini del presente regolamento, la sua manutenzione, il suo finanziamento e la sicurezza dei dati. La piattaforma ODR è di facile impiego. Lo sviluppo, il funzionamento e la manutenzione della piattaforma ODR assicurano, nei limiti del possibile, la tutela della vita privata fin dalla fase di progettazione («privacy by design») e l'accessibilità e l'utilizzabilità della piattaforma stessa da parte di tutti, comprese le persone vulnerabili («design for all» — progettazione universale)".*

2020[99]. In particolare, nell'Allegato numero 1, il Consiglio Europeo fissa le grandi linee delle attività future e afferma di perseguire l'obiettivo di garantire la privacy e la libertà e che per poterlo fare nella società digitale è necessario sviluppare per i nuovi prodotti e servizi delle strategie e delle tecnologie che siano basate sul principio di privacy by design[100].

Ancora più recente è l'articolo 12 del Regolamento del Parlamento Europeo e del Consiglio del 23 luglio 2014 n. 910 in materia di identificazione elettronica e di servizi fiduciari per le transazioni elettroniche nel mercato interno, il cui dispositivo prevede i criteri per l'interoperabilità dei regimi nazionali, tra i quali la facilitazione dell'applicazione del principio di tutela della vita privata fin dalla progettazione[101]. Ciò significa che i sistemi e le tecnologie per l'identificazione elettronica nelle transazioni online dovranno essere configurati in modo da interagire e funzionare in compatibilità tra di loro e poi dovranno tendere ad una protezione dei dati personali coinvolti che sia by design.

In ultimo è opportuno menzionare la Decisione del Parlamento Europeo e del Consiglio del 15 maggio 2014 n. 554 relativa alla partecipazione dell'Unione al programma di ricerca e sviluppo a sostegno di una vita attiva e autonoma avviato congiuntamente da più Stati membri si indicano gli obiettivi del programma "*active and assisted living*", che è volto alla creazione di migliori condizioni di vita per gli anziani e all'aumento delle loro potenzialità attraverso l'utilizzo delle tecnologie ICT, tra le cui finalità si riscontrano anche qui la

[99] Sul sito che si indica è possibile leggere tutti i progetti finanziati in Italia: <http://www.horizon2020news.it/>.

[100] Cfr. Allegato n. 1, punto 7.6, della Decisione del Consiglio del 3 dicembre 2013 n. 743 che stabilisce il programma specifico di attuazione del programma quadro di ricerca e innovazione (2014-2020) – Orizzonte 2020 e abroga le decisioni 2006/971/CE, 2006/972/CE, 2006/973/CE, 2006/974/CE e 2006/975/CE: *"Garantire la privacy e la libertà, anche su internet, e rafforzare la comprensione, da un punto di vista sociale, giuridico ed etico, di tutti i settori della sicurezza, del rischio e della relativa gestione. Al fine di salvaguardare il diritto fondamentale alla protezione della vita privata anche nella società digitale è necessario sviluppare strategie e tecnologie basate sul principio "privacy-by-design", ossia rispetto della vita privata insito nella concezione stessa alla base di nuovi prodotti e servizi. Saranno elaborate tecnologie che consentano agli utenti di controllare i loro dati personali e l'uso che ne viene fatto da parte di terzi ed anche strumenti per individuare e bloccare i contenuti illegali e le violazioni dei dati in modo da proteggere i diritti umani on-line, evitare che i comportamenti individuali o collettivi siano limitati da attività illecite di ricerca o definizione di profili […]"*.

[101] Cfr. Co. 3, lett. c), Art. 12, Regolamento del Parlamento Europeo e del Consiglio del 23 luglio 2014 n. 910 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.: *"1. I regimi nazionali di identificazione elettronica notificati a norma dell'articolo 9, paragrafo 1, sono interoperabili. 2. È istituito un quadro di interoperabilità ai fini del paragrafo 1. 3. Il quadro di interoperabilità risponde ai seguenti criteri: a) mira a essere neutrale dal punto di vista tecnologico e non comporta discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro; b) segue, ove possibile, le norme europee e internazionali; c) facilita l'applicazione del principio della tutela della vita privata fin dalla progettazione (privacy by design); […]".*

protezione e la sicurezza dei dati personali mediante l'applicazione di strumenti all'avanguardia per la tutela della vita privata fin dalla fase di progettazione[102].

Rimanendo in Europa, ma cambiando tipologia di fonte analizzata, si possono segnalare alcune delle molte comunicazioni della Commissione Europea, la quale negli ultimi anni ha ricoperto il ruolo di attrice protagonista nel palcoscenico della storia della privacy by design.

Già prima della proposta di regolamento del 2012 la Commissione ha difatti espresso la necessità di un'applicazione generalizzata del principio, come mezzo possibile per far rispettare il diritto fondamentale alla riservatezza e alla tutela dei dati personali e creare la fiducia dei cittadini europei nei confronti dell'era digitale[103]. Non solo, si è altresì impegnata a seguire l'approccio nello sviluppo di nuovi strumenti legali sfruttando le stesse tecnologie dell'informazione per integrare la protezione dei dati alla base tecnologica[104].

Nell'attesa della elaborazione dell'articolo 25 del GDPR la Commissione ha peraltro proposto l'introduzione del principio in materia di sicurezza dei dati, definendolo come la miglior strategia per potenziarla; in particolare, ha espresso la speranza che si elaborasse in materia una norma regolatoria a cui le società avrebbero potuto aderire volontariamente senza obblighi e che si

---

[102] Allegato 1, Decisione del Parlamento Europeo e del Consiglio del 15 maggio 2014 n. 554 relativa alla partecipazione dell'Unione al programma di ricerca e sviluppo a sostegno di una vita attiva e autonoma avviato congiuntamente da più Stati membri: *"1. Il programma AAL persegue i seguenti obiettivi: 1.4. sviluppare soluzioni con un buon rapporto costi-benefici, accessibili e, se del caso, efficienti sotto il profilo energetico, definendo anche le relative norme di interoperabilità e promuovendo la localizzazione e l'adattamento di soluzioni comuni che siano compatibili con le diverse preferenze sociali, i fattori socioeconomici (comprese la povertà energetica e l'inclusione sociale), le questioni di genere e i diversi aspetti regolamentari a livello nazionale o regionale, rispettino la vita privata e la dignità degli adulti più anziani, compresa la protezione e la sicurezza dei dati personali mediante l'applicazione di strumenti all'avanguardia per la tutela della vita privata fin dalla fase di progettazione ("privacy-by-design"), e, se del caso, facilitino l'accesso ai servizi nelle zone rurali e periferiche o siano disponibili per altre categorie di persone, come le persone con disabilità. Per migliorare l'accessibilità il concetto di "progettazione universale" (Design for All) sarà promosso nella messa a punto e nella diffusione delle soluzioni".*

[103] Si veda la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni "un'agenda digitale europea" COM (2010) 245, 18: *"2.3. Fiducia e sicurezza. Gli europei non adotteranno una tecnologia di cui non si fidano. L'era digitale non è sinonimo di "grande fratello" né di "cyber far west". Il diritto alla riservatezza e alla tutela dei dati personali è un diritto fondamentale nell'UE che deve essere fatto rispettare, anche online, con tutti i mezzi possibili: dall'applicazione generalizzata del principio di "privacy by design" nelle TIC pertinenti fino ad arrivare, se necessario, ad azioni dissuasive".*

[104] Si veda la Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia, COM (2010) 385, 27: *"Nello sviluppare nuovi strumenti basati sull'uso delle tecnologie dell'informazione, la Commissione si impegnerà a seguire l'approccio privacy by design (tutela della vita privata fin dalla progettazione). Per questo sarà necessario integrare la protezione dei dati personali nella base tecnologia dello strumento proposto, limitando il trattamento a quanto necessario per conseguire l'obiettivo proposto e garantendo l'accesso solo a determinati organismi in funzione della "necessità di conoscere".*

creasse una pressione tra gli operatori economici. Questa auto-regolamentazione avrebbe operato come una ISO 900021, ossia come l'insieme di norme che garantiscono la qualità della gestione organizzativa in un'azienda[105].

Durante il periodo di redazione del nuovo Regolamento, l'organo esecutivo europeo ha spiegato che il rispetto della futura norma sulla tutela della vita privata fin dalla progettazione garantirà che i prodotti e i servizi di sicurezza dell'Unione Europea rispettino i diritti degli individui e che in tal modo si potrà potenziare la fiducia dei consumatori, il cui risvolto economico non può che essere caro a Bruxelles[106]. Infine, la stessa Commissione ha da poco ribadito che oggi la pbd e la privacy by default sono dei principi che informano le norme europee sulla protezione dei dati[107].

A questo punto è opportuno concentrare lo sguardo sul nostro Paese, per completare l'analisi storica del principio. Innanzitutto, non si può che dar conto dell'importanza del principio di necessità nel trattamento dei dati nel Codice Privacy, che è una novità tutta italiana, come si è già detto, e potrebbe essere letto come un strumento normativo precursore dell'attuale articolo 25, seppur del tutto inconsapevole e, in aggiunta, come una soluzione coerente con la materia disciplinata, rendendola insuscettibile all'apprezzamento secondo una dinamica di mercato e più attenente alla protezione della personalità[108].

---

[105] Si veda la Comunicazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale Europeo, "Politica industriale della sicurezza, Piano d'azione per un'industria della sicurezza innovativa e competitiva", COM (2012) 417, 13-14: *"Da una parte, trasporre considerazioni di tipo sociale in requisiti tecnologici è estremamente difficile e reso ancor più complicato dalla grande varietà di prodotti della sicurezza presenti sul mercato. Dall'altra, le questioni sociali connesse alla sicurezza variano considerevolmente da uno Stato membro all'altro. La Commissione ritiene perciò che la strategia migliore sia l'introduzione del concetto di "tutela della vita privata fin dalla progettazione" (privacy by design) e di "tutela della vita privata per impostazione predefinita" (privacy by default) fin dalla fase progettuale. A tal fine l'operatore economico che desideri che il proprio processo di produzione venga riconosciuto come conforme al principio della "tutela della vita privata fin dalla progettazione" dovrebbe rispettare una serie di requisiti definiti da una specifica norma UE, che sarà volontaria. La Commissione è tuttavia convinta che vi sarà una forte pressione fra pari perché le aziende seguano tale norma, che dovrebbe acquisire un valore di riconoscimento simile, ad esempio, alla norma di gestione ISO 900021".*

[106] Si veda la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, "Agenda europea sulla sicurezza", COM (2015) 185, 13: *"Recentemente la Commissione ha incaricato gli organismi europei di normalizzazione di elaborare una norma sulla "tutela della vita privata fin dalla progettazione" (privacy by design) intesa a promuovere l'integrazione di standard elevati di sicurezza e dei diritti fondamentali nelle primissime fasi dei progetti tecnologici. Il rispetto di questa norma garantirà che i prodotti e i servizi di sicurezza dell'UE rispettino i diritti delle persone, rafforzando così la fiducia dei consumatori".*

[107] Si veda la Comunicazione della Commissione al Parlamento Europeo e al Consiglio "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza", COM (2016) 205, 5: *"La "protezione dei dati fin dalla progettazione" e la "protezione dei dati di default" sono ora principi che informano le norme dell'UE sulla protezione dei dati".*

[108] MANTELERO, *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, cit., 677.

Per l'appunto l'articolo 3 del D. Lgs. 196/2003, con poco più di una decina di anni di anticipo rispetto al GDPR, ha previsto che i sistemi informativi e i programmi informatici debbano essere "configurati" riducendo al minimo l'utilizzazione di dati personali e di dati identificativi. Questa configurazione può essere intesa come una progettazione, una necessaria azione concreta da parte del tecnico che deve poter escludere il trattamento di dati quando le finalità che esso persegue possono essere realizzate mediante l'utilizzo di dati anonimi o altre opportune modalità che non permettano di identificare l'interessato se non in caso di necessità. Ciò che emerge dal dispositivo è la presenza di un obbligo a tutelare il principio di minimizzazione anche tramite il design dei programmi informatici[109].

Si può interpretare la norma, quindi, come un vero e proprio strumento che prescrive l'adozione di misure tecniche. Il nostro legislatore ha affidato alla tecnologia stessa il compito di assicurare il perseguimento degli obiettivi che le norme si prefiggono: si può ben dire che la tecnologia deve incorporare la regola[110].

Nella ricerca di una connessione italiana con la pbd non si dimenticano poi le misure minime di sicurezza previste dall'articolo 33 del Codice Privacy, che ne prescrive l'adozione al fine di garantire un livello minimo di protezione dei dati personali[111]. La suddetta scelta del legislatore e l'insieme delle norme sulla sicurezza mostrerebbero ancor di più l'opportunità di avvalersi della tecnologia per creare contesti operativi conformi al dettato normativo[112].

Pensando però alla norma chiave sulla conformazione, l'articolo 3 è stato da sempre poco applicato, a causa della sua natura di norma senza una sanzione; il fatto di essere un principio guida del Codice Privacy e di non avere in sé la prescrittività che si auspica, lo rende inevitabilmente meno spendibile in un'aula giudiziaria. Tuttavia, si possono citare due esempi in cui il principio di necessità è stato utilizzato da un giudice per stabilire l'illecita violazione del diritto alla riservatezza. In un'ordinanza del 2009 il Tribunale di Nola, in un procedimento civile cautelare che riguardava un sistema di videosorveglianza installato su delle aree comuni di un condominio, ha deciso sulla rimozione delle telecamere perché non necessarie, sproporzionate rispetto alle ragioni di tutela della sicurezza e contrarie alla normativa di settore, anche con riferimento ad una delibera del Garante Italiano del 29 aprile 2004, la quale statuisce che

---

[109] PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 206.

[110] PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., 71.

[111] Cfr. Art. 33, D. lgs. n. 196/2003: *"1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali".*

[112] MANTELERO, *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, cit., 682.

se non è osservato il principio di necessità, le installazioni e l'attività non sono lecite[113]. In un ambito del tutto diverso si è pronunciato di recente il Tribunale di Bari, in un procedimento sui danni provocati dalla divulgazione di dati di un cittadino da parte di un Comune. Pur non essendoci in questo caso il nesso di causalità tra il comportamento del Comune e la condizione di malattia lamentata dall'attore, prodotta invece da attività intimidatorie dei suoi concittadini, il giudice pugliese ha affermato che l'Ente Territoriale avrebbe dovuto tenere conto dei principi fondamentali posti a tutela della privacy, ossia il principio di necessità e il principio di pertinenza, completezza e non eccedenza e così omettere la diffusione delle generalità dell'individuo[114].

In breve, operando un confronto tra il principio di necessità di cui all'articolo 3 ed e il principio di tutela della vita privata fin dalla progettazione dell'articolo 25 del GDPR, in vista della futura applicazione del Regolamento e della opportuna compatibilità delle due norme, si può notare che se il primo riguarda solo il momento precedente al trattamento, ossia la configurazione dei sistemi, il secondo è più ampio e andrà applicato ex ante e durante tutto il ciclo di vita delle informazioni. In aggiunta, l'articolo 3 è sì un principio generale, senza criteri direttivi, ma sembra riferirsi solo a situazioni in cui entra in gioco l'identificazione dell'interessato, mentre l'articolo 25 è più specifico nel dettagliare ciò che si deve tenere conto per poterlo applicare, come lo stato dell'arte e i costi di attuazione, che potrebbero costituire dei limiti, però è largamente applicabile a molte più situazioni e introduce la necessità di misure tecniche e organizzative che devono essere adeguate, parametro invece non presente nel Codice. Oltre a tutto ciò, il GDPR offre dei validi strumenti per implementare il suo principio, la certificazione e i codici di condotta, al contrario del Codice, che rimane aperto, ma più generale e soprattutto non prevede una sanzione per la sua violazione, come quella amministrativa disposta dal legislatore europeo.

---

[113] Tribunale Nola, sez. II, 03/02/2009, ord. ud. 03/02/2009 in De Iure: <https://www.iusexplorer.it/Dejure/Sentenze?idDocMaster=1998300&idDataBanks=6&idUnitaDoc=0&nVigUnitaDoc=1&pagina=0&NavId=514469624&pid=19>.

[114] Tribunale Bari, 11/01/2016, n. 73, in De Iure, <https://www.iusexplorer.it/Dejure/Sentenze?idDocMaster=4901195&idDataBanks=6&idUnitaDoc=0&nVigUnitaDoc=1&pagina=0&NavId=526920785&pid=19>: "*È pur vero che il Comune, nell'ambito dell'esercizio di un'attività istituzionale, oltretutto obbligatoria, avrebbe dovuto tener conto dei principi fondamentali posti a tutela della privacy, e cioè il principio di necessità, "riducendo al minimo l'utilizzazione di dati personali e di dati identificativi" (art. 3 del D.L.gs. n. 196/2003), ed il principio di pertinenza, completezza e non eccedenza, utilizzando soltanto quei "dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto" (art. 11 del D.L.gs. n. 196/2003), considerato che le ordinanze notificate a soggetti diversi dal D. avrebbero condotto allo stesso risultato anche con l'omissione del nome dell'odierno attore e del riferimento alla missiva inviata dal suo legale, ma, ciò nonostante, si ribadisce come l'attore abbia richiesto il risarcimento in funzione non già di un illecito trattamento dei dati e, quindi, di violazione della privacy, bensì di una patologia neurologica conseguente allo stato d'ansia generato dalle minacce poste in essere da terzi, mai identificati".*

Al di là di ogni critica, che contesta il costo esorbitante per le imprese o la limitazione della libertà individuale ed economica, il principio di necessità si è rivelato un principio generale per lo sviluppo tecnologico, che ha spinto e tuttora spinge verso la minimizzazione dell'utilizzo dei dati personali e di quelli identificativi, basandosi sulla considerazione che si possono evitare alcuni rischi di sicurezza solo se si implementano i requisiti legali durante la programmazione dell'architettura tecnologica[115]. Quelle libertà non sono limitate, sono invece ancora più protette grazie alla tecnologia, la quale di per sé non può eliminare i problemi in materia di privacy, però rende possibili i vari meccanismi che la proteggono grazie all'incorporazione delle sue regole[116].

Per quanto riguarda invece il concetto di privacy by design in Italia, si può citare il parere del Garante per la Protezione dei Dati Personali del 26 marzo 2015 sull'avvio della consultazione pubblica sull'Internet of Things[117]*.* L'autorità nelle premesse del suo parere spiega che in materia di protezione dei dati personali devono essere adottate le misure di sicurezza tali da evitare i rischi di interferenze ingiustificate e di manomissioni dei dati e, ancor prima, volte a minimizzarli quando possibile; con questa prospettiva e con lo scopo dichiarato di valutare i rischi del trattamento per tutto il ciclo vitale del prodotto o del servizio, il Garante afferma che è auspicabile ricercare soluzioni improntate sull'approccio di pbd[118]*.* A tal proposito, attraverso lo stesso documento, ha

---

[115] GUARDA, *Data Protection cit.,* 86: "*The data minimizing principle acts as a general principle policy for the technological development, declaring that information systems and software shall be configured by minimizing the use of personal data and identification data. Some authors claimed that this rule seems to impose an exorbitant requirement and that it aims at regulating the use of computer resources by private and public parties: that would rise manifest unconstitutionality problems with respect to the individual and company freedom. The principle under discussion, although it could appear absurd as regarding to its generic character, bases its justification on the consideration that some security risks of the computer system can be avoided only we decide to implement data protection legal requirements when programming the architecture".*

[116] *Ibidem,* 87.

[117] "Internet of Things*"* è un'espressione coniata nel 1999 da Kevin Ashton, co-fondatore dell'Auto-ID Center, un'organizzazione di ricerca globale, indipendente e no profit che ha sede presso il Massachusetts Institute of Technology. Con queste parole si intende riferirsi alla presenza di oggetti e cose che, grazie al progresso tecnologico possono interagire utilizzando la Rete e rendono la realtà costantemente connessa.

Per una più precisa definizione e un approfondimento si v. L. ATZORIA, A. IERAB, G. MORABITOC, *The Internet of Things: A survey*, *Computer Networks* 2787 (2010), 2787: *"The basic idea of this concept is the pervasive presence around us of a variety of* things *or* objects *– such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals".*

[118] Garante per la Protezione dei Dati Personali, Parere 26/03/2015, n. 3898704, "Avvio della consultazione pubblica su Internet delle cose (Internet of Things)": *"In tale prospettiva ed allo scopo, altresì, di valutare i possibili rischi del trattamento nel corso dell'intero ciclo vitale del prodotto o della fornitura del servizio l'Autorità ritiene auspicabile che fin dalla fase della progettazione dei servizi e degli oggetti destinati ad interagire nell'Internet of things gli operatori coinvolti ricerchino soluzioni improntate ad una concreta applicazione dei paradigmi e delle strategie basate sul cd. approccio di privacy and data protection by design".*

deliberato l'avvio di una consultazione pubblica per acquisire delle osservazioni e delle proposte sugli aspetti elencati nel parere, compresa l'applicabilità del paradigma di privacy by design. Si può dunque notare che il tema della presente tesi è anche oggetto di attuale riflessione da parte della nostra Autorità Garante.

4. Il concetto di privacy by design e i suoi vantaggi

La privacy by design garantisce una tutela proattiva mediante l'inserimento nei prodotti e nei servizi informatici di strumenti di protezione sin dalla fase di progettazione. Il concetto è così caratterizzato da una netta tensione preventiva ed onnicomprensiva, in modo da affrontare anche le minori invasioni della sfera di personalità dell'individuo[119].

In questo paragrafo si mira a delineare in modo approfondito quali siano i vantaggi e gli aspetti che contraddistinguono l'approccio oggetto della presente tesi, attraverso vari contributi dottrinari provenienti soprattutto da oltreoceano e appartenenti a giuristi, economisti, ingegneri e ad informatici.

Si può affermare, come è stato fatto dall'European Union Agency for Network and Information Security (d'ora in avanti ENISA), un'agenzia dell'Unione Europea che si occupa di sicurezza delle reti e dell'informazione, che la pbd è un concetto sfaccettato, perché è stato descritto dal mondo del diritto come un principio generale dai contorni molto ampli ed indefiniti e dai computer scientists e dagli ingegneri come l'utilizzo delle tecniche protettive della privacy dette PETs, anche se in realtà non è né impreciso, né riducibile a queste[120]; consiste, invece, in un processo che coinvolge varie componenti tecnologiche ed organizzative, sia il diritto che l'informatica, ed applica i principi della privacy e della protezione dei dati personali[121].

---

[119] In tal senso, PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 200.

[120] Le *Privacy Enhancing Technologies* (PETs) sono varie tipologie di tecnologie che mirano alla protezione della *privacy* e che sono state sviluppate a partire dagli anni Novanta del secolo scorso. Nella Comunicazione della Commissione al Parlamento Europeo e al Consiglio sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET), COM (2007) 228, si legge che esempi di PETs sono il ripristino automatico dell'anonimato dopo un determinato periodo di tempo o degli strumenti di crittaggio volti a prevenire la pirateria informatica e che lo sviluppo di questi strumenti è fondamentale e necessita di essere promosso, anche da parte delle autorità pubbliche. Le varie tecnologie si differenziano per molti aspetti, ma in generale si può affermare che sono dei rimedi successivi e non proattivi, la cui efficacia è stata limitata e non sufficiente a garantire la *privacy* in relazione allo sviluppo dei sistemi ICT.

[121] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *Privacy by design in big data, an overview of privacy enhancing technologies in the era of big data analytics*, 2015, 21: *"Nowadays, it is regarded as a multifaceted concept: in legal documents on one hand, it is generally described in very broad terms as a general principle; by computer scientists and engineers on the other hand it is often equated with the use of specific privacy enhancing technologies. However, privacy by design is neither a collection of mere general principles nor*

Innanzitutto va specificato che la privacy by design si inserisce all'interno di una proposta più ampia, definita value sensitive design (VSD), la quale è basata teoricamente su un tipo di design della tecnologia che rappresenta dei valori umani attraverso il suo sviluppo e progetto, in una modalità orientata ai principi ed onnicomprensiva, che sappia tener conto ad esempio del benessere, della dignità, della giustizia, dello stato sociale, dei diritti umani e della privacy[122]. Insomma, si tratta della concettualizzazione di una tecnica di design piuttosto ambiziosa e impegnativa.

La pbd è quindi una realizzazione di valori e nello specifico dei principi della materia e delle norme che regolano la privacy attraverso un design fisico, ossia a specificazioni tecniche, all'architettura e al codice dello strumento, con lo scopo di materializzare questi valori e renderli operanti nella realtà[123].

Un autorevole contributo statunitense spiega che i valori di VSD sottesi alla privacy by design sono i Fair Information Practices (d'ora in avanti FIPs), ossia quel complesso di principi e standard internazionalmente riconosciuti in materia di protezione dei dati personali[124]. I FIPs cambiano in base agli ordinamenti giuridici e sono ancorati alle normative di riferimento: in Europa si guarda alla Direttiva 95/46 (e in futuro al GDPR), negli Stati Uniti al lavoro di sistematizzazione degli statutes settoriali compiuto dalla dottrina e dalla FTC. Per avere una visione generale si può prendere a modello le linee guida della OECD, che condensano le varie proposte a livello internazionale. Primariamente i FIPs sono stati elaborati dal Report del 1973 del Secretary Advisory Committee del Dipartimento degli Stati Uniti per la salute, l'educazione

---

can it be reduced to the implementation of PETs. In fact, it is a process involving various technological and organizational components, which implement privacy and data protection principles".

[122] D. K. MULLIGAN, J. KING, *Bridging the gap between privacy and design*, 14 *U. Pa. J. Const. L.* 989 (2012), 1019: *"Privacy by design, as we re-envision it, should aim to identify contextually-bound understandings of privacy, and, to design system architectures, interfaces, default settings as well as corporate policies that reflect them. Thus understood, privacy by design fits under the broad umbrella of VSD (Value Sensitive Design), a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process." VSD research has focused on a broad set of values, including well-being, dignity, justice, welfare, human rights, and privacy".*

[123] Una definizione molto chiara e suggestiva è contenuta in D. KLITOU, *Privacy-Invading Technologies and Privacy by Design, Safeguarding Privacy, Liberty and Security in the 21st Century*, T.M.C. Asser Press, 25 Information Technology and Law Series, Hague (2014), 262: *"Pbd is the realization of values, in this case the principles of privacy and corresponding rules/regulations, via the physical design, technical specifications, architecture and/or computer code of the device, system, technology or service concerned, where applicable. The aim of PBD is to design and develop a system or device (i.e. software and/or hardware) in a way that supports and materializes those principles, values and rules as goals and functions, whereby that system or device then become "privacy-aware" or "privacy-friendly".*

[124] I. S. RUBINSTEIN, N. GOOD, *Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents*, 28 *Berkeley Tech. L.J.* 1333 (2013), 1337: *"An obvious starting point for understanding what it means to design products and services with privacy in mind is the set of internationally recognized values and standards about personal information known as the Fair Information Practices ("FIPs")".*

e il welfare intitolato *Records Computers and the Rights of citizens*. All'epoca furono delineati cinque principi FIPs, dai quali non era possibile trovare eccezione a meno che non si provassero degli interessi significativi dell'interessato al trattamento o degli interessi sociali di primaria importanza, già previsti dalla legge; in particolare i principi del 1973 sono i seguenti:

1. Non deve esserci sistema di raccolta dei dati personali la cui esistenza sia segreta;
2. Deve esserci un modo per l'individuo di sapere quali informazioni su di lui siano state raccolte e come siano utilizzate;
3. Deve esserci un modo per l'individuo di impedire che le informazioni ottenute per uno scopo preciso siano utilizzate o rese disponibili per altri scopi senza il suo consenso;
4. Deve esserci un modo per l'individuo di correggere o emendare una sua informazione identificativa registrata;
5. Ogni organizzazione che crea, mantiene, utilizza e distribuisce raccolte di dati personali identificativi deve assicurare l'affidabilità dei dati per lo scopo prefissato e deve prendere delle precauzioni ragionevoli per prevenire l'abuso delle informazioni[125].

Pochi anni dopo l'OECD ha definito con puntualità i suddetti FIPs come: "collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability"[126].

Perciò, quando si dichiara che la pbd consente l'inserimento delle regole della privacy all'interno dei sistemi informatici, si intende considerare allo stadio

---

[125] U.S. Department of Health, Education & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Records Computers and the Rights of citizens*, 1973, 41: "*Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice".*

-There must be no personal-data record-keeping systems whose very existence is secret.

-There must be a way for an individual to find out what information about him is in a record and how it is used.

-There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

-There must be a way for an individual to correct or amend a record of identifiable information about him.

-Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

These principles should govern the conduct of a personal-data record-keeping systems. Deviations from them should be permitted only if it is clear that some significant interest of the individual data subject will be served or if some paramount societal interest can be clearly demonstrated; no deviation should be permitted except as specifically provided by law".

[126] Cfr. OECD Guidelines on the Protection of privacy and transborder flows of personal data, in the form of a Recommendation by the Council of the OECD, 23 September 1980, par. 7, in Rete:
<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

del design le limitazioni previste dalla legge e il cuore dei principi della materia, per lo più identificati dai Fair Information Practises. Per meglio identificarli in prospettiva concreta e, a parere di chi scrive, consentire l'applicazione della metodologia pbd in modo uniforme ed equivalente in più ordinamenti con differenti basi giuridiche e così avvantaggiare lo scambio transfrontaliero dei dati e, perché no, non penalizzare il mercato internazionale dei servizi e prodotti, che con l'era digitale ha assunto proporzioni mondiali, si intende utilizzare la versione dei FIPs elaborata da due autori statunitensi, i quali hanno compiuto una ricerca sulle varie formulazioni provenienti da diversi contesti ed hanno creato un elenco di nove principi largamente condivisibili. Di seguito vengono riportati in traduzione:

1. Limiti definiti per i titolari e gli incaricati nella raccolta, nel trattamento e nell'utilizzo dei dati personali (principio di minimizzazione dei dati);

2. Qualità del dato (accuratezza, completezza e puntualità);

3. Limiti alla conservazione dei dati;

4. Notifica agli utenti individuali;

5. Scelta individuale o consenso riguardante la raccolta e il conseguente utilizzo delle informazioni personali;

6. Ragionevole sicurezza dei dati conservati;

7. Trasparenti processi di trattamento che gli utenti coinvolti possono facilmente capire e verso i quali possono agire;

8. Accesso ai propri dati personali;

9. Applicazione dei diritti e degli standard sulla privacy (comprendenti l'autoregolamentazione delle aziende, le misure organizzative applicate dalle imprese, la vigilanza regolatoria e il contenzioso civile)[127].

Se si dovesse applicare invece la pbd in Italia si dovrebbe tenere conto dei principi europei contenuti nelle direttive e soprattutto del nostro Codice Privacy. Perciò si utilizzerebbero: il principio di necessità nel trattamento dei dati, "*the principle of lawful processing, the principle of purpose specification*

[127] RUBINSTEIN, GOOD, *Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents*, cit., 1343: *"There are many different formulations and they vary in crucial respects. The different versions coalesce around the following nine principles:*
1. Defined limits for controllers and processors of personal information on the collection, processing, and use of personal data (often referred to as data minimization);
2. Data quality (accurate, complete, and timely information);
3. Limits on data retention;
4. Notice to individual users;
5. Individual choice or consent regarding the collection and subsequent use of personal information;
6. Reasonable security for stored data;
7. Transparent processing systems that affected users can readily understand and act on;
8. Access to one's personal data; and
9. Enforcement of privacy rights and standards (including industry self-regulation, organizational measures implemented by individual firms, regulatory oversight and/or enforcement, and civil litigation)".

and limitation, the data quality principles (relevancy of data, accuracy of data), limited retention of data, exemption for scientific research and statistics, the principle of fair processing, the principle of accountability"[128]. Dal 25 maggio 2018 diventeranno operativi anche i principi del GDPR e così, ad esempio l'articolo 5 rubricato proprio "principi applicabili al trattamento di dati personali"[129].

Prendendo ora in considerazione il momento applicativo del principio in questione, si può citare il contributo di altro autore statunitense, il quale ha precisato che la Rete è pervasa da norme commerciali definite "non-privacy", cioè che spingono le imprese a sfruttare i dati raccolti in un modo eticamente scorretto, e che per far fronte ai rischi dovuti alle moderne tecnologie è necessario tenere bene a mente il fattore temporale di intervento, ossia la tempistica nella previsione degli strumenti che limitino questi comportamenti abusivi. A tal proposito, sembra assumere grande importanza l'influenza delle norme sociali, liberamente createsi in un contesto, le quali poi tendono a tradursi in regole tecniche quando si crea l'aspettativa negli individui; le regole che vengono poste in essere tramite l'architettura della tecnologia sono fondamentali e la stessa può essere modellata per proteggere la privacy sia nel periodo iniziale della sua costruzione sia in uno stadio successivo, quando il prodotto o il servizio sono già in circolazione[130].

Quindi, la privacy by design può riguardare sia delle tecnologie nuove, sia quelle già presenti e più o meno datate, anche se, come è ovvio, l'adattamento di queste al principio comporterà delle fatiche maggiori per gli addetti ai lavori.

---

[128] Si veda il lavoro approfondito contenuto in European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European data protection law,* 2014, 61, in Rete: <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law>.

[129] Cfr. Art. 5, Reg. 2016/679: *"1.I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). 2.Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)".*

[130] Si veda la riflessione accurate contenuta in G. BERNSTEIN, *When new technologies are still new: windows of opportunity for privacy protection*, 51 *Vill. L. Rev.* 921 (2006), 947-948.

Per l'appunto, si è stimato che più sono complesse e ambiziose le esigenze di privacy, prima si dovranno introdurre nel processo di sviluppo del software le considerazioni e le specificazioni necessarie[131].

Nel complesso, pbd significa prima di tutto sicurezza dei dati personali e poi garanzia della raccolta e del trattamento del minor numero di dati possibile[132].

Uno dei maggiori vantaggi è la prevenzione: le violazioni e i danni vengono limitati sia da parte dei titolari dei trattamenti sia dagli utenti stessi. Un'interessante riflessione che considera il design di un sito web come un elemento contrattuale del "prodotto" digitale utilizzato dall'utente, suscitando alla scrivente delle riflessioni sulla possibilità di una responsabilità contrattuale del gestore in caso di inadeguatezza del trattamento per i difetti di design, asserisce che un prodotto ben progettato dissuade o previene gli utilizzi rischiosi e rende prevedibili le loro conseguenze[133].

Oltre alla prevenzione, si ottiene una maggiore effettività delle norme giuridiche, che vengono tradotte in un linguaggio capibile dalla macchina (*legal machine language*) e vengono poste in essere eccezionalmente ex ante. In materia il focus non è più solo sul diritto, e sui suoi operatori, ma si sposta sui tecnici, informatici, ingegneri, sviluppatori, e lì si concentra[134].

Ciò che si vuole prontamente specificare è che la privacy by design non intende creare delle barriere allo sviluppo tecnologico, limitare l'innovazione e il progresso; essa mira, invece, a svolgere la funzione di guida prudente e controllata[135]. Operando infatti un bilanciamento tra la libertà di iniziativa economica e la libertà di innovazione, da un lato, e la protezione della privacy, che significa garanzia della libertà degli individui e della società, dall'altro, può essere chiesto alla tecnologia di non operare indiscriminatamente. Un esempio concreto in un altro contesto è la progettazione delle automobili: i limiti di velocità vengono inseriti nel motore e nei cavalli per impedire ai conducenti di

[131] È di questa opinione D. W. SCHARTUM, *Making privacy by design operative*, 24 *IJLT* 151 (2016), 155.
[132] Il contributo che spiega in questi termini la *privacy by design* attraverso l'ausilio di strumenti concreti è fornito da P. SCHAAR, *Privacy by Design*, 3 *IDIS* 267 (2010).
[133] J. GRIMMELMANN, *Privacy as product safety*, 19 *Widener L.J.* 793 (2010), 821: *"For one thing, good product design discourages or prevents particularly hazardous uses. For another thing, good product design makes consequences predictable".*
[134] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 263: *"The focus on privacy law and the burden of compliance, responsibility, or liability are, therefore, shifted to the designers/engineers and manufactures/developers of the technologies (software or hardware) concerned and further away from the operators or controllers of these technologies and/or the application service providers".*
[135] *Ibidem,* 264: *"In essence, PBD is meant to serve not as a barrier to technology, but rather as a guided and prudent driver of technological development".*

andare oltre e rischiare malauguratamente la propria incolumità[136]. In questo modo si dà un'etica alla tecnologia e a farlo è proprio il diritto. Si è scritto, infatti, che l'approccio di pbd consiste nel partire dalle leggi, i regolamenti, i principi, le norme e le libertà che regolano in comportamento umano e garantiscono agli individui di godere di alcuni diritti e libertà, e giunge alla realizzazione di soluzioni che minimizzano le intrusioni su di esse e le implementino il più possibile[137].

L'efficacia di una previsione preventiva delle misure attuabili è assicurata solo se la tecnologia progettata non sia aggirabile o quantomeno sia estremamente arduo poterlo fare, escludendo i comportamenti criminosi, per i quali si entra in un altro campo del diritto e in relazione ai quali devono essere poste in essere le azioni previste dalla ricerca sul diritto penale dell'informatica[138]. Le soluzioni di pbd sarebbero meno aggirabili di altre tecnologie come le PETs perché sono pensate per essere tendenzialmente uniche e sono realizzate su misura del particolare sistema coinvolto, rendendole non generalizzate e non rigide[139].

Si è soprattutto riflettuto sull'inserimento di limitazioni tecnologiche nei prodotti, ma la privacy by design non si limita solo a questo. La metodologia proattiva opera anche in ambito organizzativo e manageriale, come è evidente da ultimo dalla previsione normativa dell'articolo 25 del GDPR, richiedendo ai titolari del trattamento di adottare misure procedurali. Questa caratteristica differenzia ancora una volta la pbd dalle PETs e, a parere della creatrice di questo concetto, Ann Cavoukian, ciò dimostra la sua natura di soluzione

[136] L'esempio ha preso spunto dall'analogia creata sulle automobili contenuta nel testo appena citato, ma si tratta di un'idea della Royal Academy of Engineering.

[137] *Ibidem,* 267: *"Essentially the overall objectives and approach of PBD is to go from written privacy/data protection laws, regulations, privacy principles, norms and civil liberties that regulate human behavior and grant individuals' certain rights/freedoms to the realization of technological/design solutions that minimize the intrusive capabilities of a device, product or service and implement those laws and principles".*

[138] In questo campo la tipica funzione deterrente è svolta dalla previsione di pene in relazione a delle condotte contraddistinte da una certa antigiuridicità. A titolo di esempio l'articolo 169 del Codice Privacy punisce con l'arresto sino a due anni chiunque che, essendovi tenuto, omette di adottare le misure minime di sicurezza previste dall'articolo 33 dello stesso Codice. Si tratta di un reato omissivo proprio che si consuma nel momento in cui si inizia il trattamento dei dati personali senza adottare le misure minime di sicurezza. Il soggetto attivo è perciò il titolare del trattamento. Nel secondo comma dell'articolo 169 si statuisce che può essere impartito un termine per adeguarsi seguendo delle istruzioni e se ciò è compiuto il reato può estinguersi con il pagamento di una quota della sanzione amministrativa, il che è un tipico meccanismo del diritto penale premiale.

[139] *Ibidem,* 271: *"On the other hand, the circumvention of PBD solutions is essentially meant to be (practically) impossible or exceptionally difficult, since it would mean attempting to force the device/system concerned to perform an act it is not designed or engineered to do or is not capable of doing (in its present form). Another difference of PBD solutions from PETs is that the design/architectural and technical solutions are normally unique and tailored to the particular system, technology or device concerned".*

onnicomprensiva e il fatto di essere il prossimo passo nell'evoluzione della discussione sulla privacy[140].

Inoltre, può delinearsi il vantaggio di generare una maggiore fiducia nei consumatori dei prodotti e dei servizi informatici, aspetto la cui presenza è di fondamentale importanza in un mercato di portata globale. Si è detto che una gestione responsabile delle informazioni, che includa una attenzione accurata alla protezione delle informazioni personali, contribuisce infatti alla creazione e al mantenimento di una relazione commerciale di successo nel nuovo mondo digitale[141].

La pbd è stata definita un concetto "good for business" dalla stessa Cavoukian e altri commentatori hanno ritenuto che generi una maggiore soddisfazione nel consumatore in termini relazionali e competitivi[142]. Tra l'altro è stato ulteriormente evidenziato che così come le aziende stanno provvedendo allo sviluppo di prodotti più compatibili con le esigenze di protezione ambientale e hanno ottenuto dei profitti grazie a degli iniziali investimenti, tanto più potranno compiere la stessa scelta di cambiamento per un nuovo design delle tecnologie che sia più privacy-friendly[143]. A ciò consegue che economicamente il consumatore aumenta la propria fiducia nel mercato dei prodotti e dei servizi, la sua aspettativa cresce, la domanda aumenta e i costi del commercio diminuiscono; sul piano giuridico, viene maggiormente tutelato un contraente che da sempre è risultato debole. L'obbiettivo perseguito dalla FTC, come si è delineato nel paragrafo ad essa dedicato, può così essere più facilmente raggiunto. Sull'argomento, un contributo dottrinario canadese sull'evoluzione della consumer privacy law riferisce che l'approccio di privacy by design ha

---

[140] A. CAVOUKIAN, *Privacy by design: the definitive workshop* - a *foreword by Ann Cavoukian*, 3 *IDIS* 247 (2010), 248: *"Where PETs focused us on the positive potential of technology, Privacy by Design prescribes that we build privacy directly into the design and operation, not only of technology, but also of operational systems, work processes, management structures, physical spaces and networked infrastructure. In this sense, Privacy by Design is the next step in the evolution of the privacy dialogue".*

[141] *Ibidem,* 249: *"Now, faced with increasingly diffused and complex relationships between consumers and the organizations they do business with, as well as new forms of interaction between organizations working together in federated models, the need for trust is greater than ever before. And yet, it is becoming more elusive and harder to earn. Responsible information management practices, including paying close attention to the protection of personal information, form an important part of building and maintaining successful relationships in this new world. In a marketplace where organizations are banding together to offer suites of goods and services, trust is clearly essential".*

[142] Si veda PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 201.

[143] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 280: *"Just as companies are increasingly realizing the "going green" and designing and manufacturing products in an environmentally-friendly manner is good for business and the investment of doing so will pay off in the long-run, so too are companies increasingly realizing that designing technologies in a privacy-friendly manner could drive their business forward and provide the products and services that both governments and consumers demand".*

riscosso un certo successo in ambito giuridico proprio per la sua capacità di adattarsi ai continui cambiamenti delle tecnologie nell'era di Internet[144]. Lo stesso autore sottolinea, però, che i millantati benefici al consumatore saranno concretizzabili solo se muta la concezione che i soggetti commerciali hanno dei dati personali, essendo molto alta la tentazione di monetizzarli e sfruttarli per ottenere ulteriore profitto. A suo avviso, essi dovrebbero focalizzarsi sul far aumentare la fiducia nelle tecnologie emergenti dato che, proteggendo maggiormente i dati dei consumatori, la regolazione giuridica, se applicata correttamente, assumerebbe un ruolo prezioso nell'avvantaggiare gli sviluppi tecnologici più in sintonia con le aspettative di tutela delle parti deboli e la ricchezza aumenterebbe[145].

Non solo: un altro beneficio consisterebbe nell'aumento della cultura della privacy degli individui, che, essendo considerati al centro e coinvolti maggiormente nelle scelte di gestione dei propri dati, hanno maggiori strumenti per essere più consapevoli e attenti sulla circolazione dei propri dati e sulla protezione della loro riservatezza. La disimmetria informativa tra individuo/utente e gestore/titolare ha spesso condotto a situazioni in cui il soggetto, ignaro di aver prestato il proprio consenso per l'utilizzo a certi fini dei propri dati o inconsapevole di avere il diritto di prestarlo, si è visto circolare informazioni personali che in realtà desiderava mantenere segrete, soprattutto nell'ambito dei social media. È all'ordine del giorno la leggerezza con la quale si accettano le condizioni contenute nelle informative per la gestione dei dati personali perché troppo lunghe, complesse e al di là della portata dell'uomo medio. Su questo, la privacy by design intende porre rimedio: si mira anche alla previsione di strumenti che rendano più chiaro e più facile all'utente/consumatore scegliere se prestare o meno il proprio consenso.

Ann Cavoukian ritiene che la pbd sia un mezzo per la diffusione di una particolare cultura di privacy, non solo tra gli individui, ma anche tra i soggetti

---

[144] M. KIANIEFF, *The evolution of consumer privacy law: how privacy by design can benefit from insights in commercial law and standardization*, 10 *CJLT* 1 (2012), 12: *"Although this is a relatively straightforward proposition, it has the potential to significantly reduce transactions costs if the privacy ramifications that flow from technological developments could be identified and corrected from the design stage before the product is released to the public rather than the present reactionary approach. The Privacy by Design approach has found a receptive audience throughout the world as policymakers debate how best to regulate the Internet following recent developments and the ever-changing nature of Internet technologies".*

[145] *Ibidem,* 22: "*Privacy by Design necessitates a re-conception of how business views personal information to remove the monetary temptations that flow from it. Instead, the focus ought to be on helping build confidence in the new emerging technologies in a manner that accord with consumer expectations. By protecting consumer information in this manner, regulation can play a valuable role in advancing the types of technological developments that are more in keeping with what consumer's desire, by reducing consumer trepidation and ensuring that vulnerable parties are protected. In this sense, a corresponding advance in confidentiality can help create the conditions that facilitate the growth of certain business relationships much the same way that the law of confidentiality has in the past".*

commerciali, dal momento che, aumentando la fiducia e l'attenzione dei consumatori, le imprese sono spinte a considerare la gestione del dato non più solo come una questione di conformità alle norme, bensì come un'opportunità di business[146]. Ovviamente i costi elevati per le aziende non sono ineliminabili, come si dirà nel paragrafo successivo.

Ulteriormente, la privacy by design è utile e positiva per la protezione dei dati personali perché aumenta il grado di sicurezza dei dati, tema che si è detto essere strettamente legato a quello della privacy. L'aumento dei security breaches negli ultimi anni è stato considerato un problema strutturale, dipendente dalla fattezza delle tecnologie ICT e di conseguenza un'importante opportunità per la pbd[147]. Una completa sicurezza dei dati è impossibile, non si può prevedere ogni possibile infrazione verificabile nell'Internet of Things, sia a livello giuridico che tecnico e così alcune trasgressioni sono e saranno sempre inevitabili; tuttavia, data la difficoltà nel rendere operative le regole di diritto contro gli hackers e i furti o gli utilizzi illeciti, si può optare per l'alternativa concreta dell'implementazione delle protezioni tecniche ed organizzative che riducano la probabilità delle violazioni di sicurezza dei dati[148]. In breve, si afferma, attraverso la pbd e le scelte architetturali il trade-off tra privacy e sicurezza è minore e meno valido[149].

---

[146] *Ibidem,* 251: *"By doing so, I believe that Privacy by Design will assist in creating a particular culture of privacy which I have been advocating for many years. This culture of privacy is what emerges when organizations approach privacy not as a compliance issue, but as a business issue. It is what takes hold when the leadership of an organization comes to see that the implementation of positive privacy controls creates—rather than constrains—business opportunities. In short, it is a culture of "win-win" or positive-sum".*

[147] P. HUSTINX, *Privacy by design: delivering the promises,* 3 *IDIS* 253 (2010), 254: *"First of all, it should be clear that the need for "Privacy by Design" could never be better illustrated than by the increasing number of data security breaches that we have seen in recent years. As far as Europe is concerned, this is not only true for the UK, but also for other EU member states. In fact, security breaches may well be a structural problem for an information society that is increasingly dependent on the good performance of ICT. This should therefore also be seen as an opportunity for Privacy by Design".*

[148] W. HARTZOG, *Reexamining privacy value: the value of modest privacy protections in a hyper social world,* 12 *Colo. Tech. L.J.* 333 (2014), 338: *"Perhaps the most promising strategy for indirect and modest privacy remedies is to focus on the design of technologies. While data security requirements might seem to companies like direct and robust regulations, they are, in effect, indirect protections against the wrongful access and use of personal information. Given the popularity of "Privacy by Design" and the proper architecture of the Internet of things, it is easy to forget that data security is the most prominent design-based approach to protecting privacy. Virtually every data security professional would likely agree that perfect security is impossible. Data breaches are inevitable. Given the difficulty in directly enforcing laws against hackers and data thieves, the next best alternative would seem to be the implementation of technical and administrative safeguards to reduce the probability of a data breach".*

[149] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 319: *"Especially, through PBD and certain choices of architectures used, the trade-off argument between privacy/liberty and security is less and less valid".*

Affinché tutto ciò sia verificabile, le norme che impongono l'applicazione dell'approccio di privacy by design dovrebbero essere vincolanti per i produttori dei sistemi ICT e non solo per i titolari del trattamento dei dati, soggetti che sono spesso differenti. Questo coinvolgimento degli sviluppatori è innovativo e difficile da attuare, ma risulta appropriato se si vuole davvero passare dalle parole ai fatti[150].

Un'altra parte della dottrina statunitense riscontra che il principio in questione sia uno strumento efficace nel prevenire le possibili cause giudiziarie in materia di privacy. I costi dei futuri contenziosi potrebbero essere evitati dall'incorporazione delle regole nella tecnologia. Si è stimato, nel campo energetico delle smart grid, che i costi legali per le imprese siano molto elevati, tanto da spingerle ad assumere delle figure professionali definite chief privacy officers per gestire al meglio il rischio giudiziario; non solo, molte società sono state indebolite e danneggiate per non aver tenuto conto dei principi della privacy nello sviluppo dei propri strumenti tecnologici[151]. Lo stesso autore puntualizza che i costi di un nuovo design su un prodotto energetico privo di qualsiasi protezione sono maggiori rispetto a quelli di una ricerca e attenzione precedente[152]. A parere di chi scrive, si può estendere la suddetta riflessione anche in altri contesti applicativi, tenendo ben presente il fatto che il rischio di una causa giudiziaria sia spesso esso stesso uno strumento utile per incoraggiare indirettamente ad una corretta gestione dei dati personali che sia conforme alla normativa.

Quando si pensa ad un'applicazione della pbd si dovrebbe evitare di ragionare per schemi rigidi e precostituiti. Il vantaggio dell'approccio è la sua adattabilità alla situazione concreta. In aggiunta, l'obbligo di implementazione

---

[150] *Ibidem,* 255: *"Finally, it would be important to include the principle of "Privacy by Design" among the basic principles of data protection, and to extend its scope to other relevant parties, such as producers and developers of ICT products and services. This would be innovative and require some further thinking, but it would be appropriate and only draw the logical consequences of a promising concept".*

[151] A. SCHIRA, *Protecting progress and privacy: the challenges of smart grid implementation*, 6 *ISJLP* 629 (2011), 652: *"Energy companies can avoid the costs of future litigation and public relations backlashes by incorporating privacy policies into their new technologies. Other industries, like the behavioral advertising market, have faced significant litigation fees as a result of privacy conflicts. The rise of such litigation has resulted in some federal policy changes that have been significant enough for companies to hire Chief Privacy Officers as legal and technological advisors. In a self-regulatory manner, creators of major websites have begun to change their policies throughout the industry to become more privacy friendly. However, these companies, and privacy rights as a whole, have been impaired because this issue was not considered early on in the development of this new technological medium".*

[152] *Ibidem,* 652: *"The creation of new legal requirements can be particularly costly for businesses in several ways. First, businesses will have to design new technologies or alter those that have already been created in order to satisfy the new regulations. New research, design, and the repair or replacement of old models could cost a significant amount if a company has not implemented any protections in the original model. Meanwhile, the time spent redesigning existing elements of the grid could have been used to further develop smart grid technologies".*

dovrebbe essere flessibile per garantire alle autorità di controllo o garanti della protezione dei dati di valutare caso per caso l'attuazione del principio[153]. Potrebbe sembrare ossimorico definire flessibile una soluzione che comporta l'utilizzo di uno strumento rigido come la tecnologia: ciò che si intende sottolineare è che la fonte sarà il diritto e l'interpretazione del principio sarà compiuta in base alla reale necessità dello specifico trattamento di quei dati personali raccolti. La tecnologia, inevitabilmente, si differenzia dal diritto perché regola il comportamento umano in modo diretto e prima del verificarsi dei fatti[154]. Eppure, se sarà compito del diritto statuire le modalità in cui la tecnologia debba svilupparsi, il problema della rigidità sarà attenuato. La legislazione non potrà riguardare ogni situazione bisognosa di tutela giuridica, ma dovrà essere flessibile, pur essendo contraddistinta dai caratteri dell'apertura, della chiarezza e dell'adattabilità al particolare sistema alla quale deve applicarsi[155]. L'interpretazione del principio potrà così cambiare in base al progresso tecnologico; in questo senso l'articolo 25 del GDPR sembra aver colto nel segno nel prescrivere la protezione della vita privata fin dalla progettazione senza limitarsi a specifiche tecniche tecnologiche. Citando un autore canadese, il diritto deve rimanere vigile per assicurare che lo sviluppo della tecnologia accresca la libertà individuale e non la diminuisca[156].

Successivamente, si può notare che un utente di un sistema informatico conformato alla pbd non solo è tutelato grazie alla garanzia di un trattamento dei suoi dati personali che sia conforme ai principi della privacy, ma anche da un maggiore controllo che lui stesso può effettuare sulle proprie informazioni divulgate. Ad esempio, nel mondo dei social network, ciò significa che si impedisce ad un soggetto di rendere pubblico inconsapevolmente delle

---

[153] In tal senso, PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 212.

[154] L. TIEN, *Architectural regulation and the evolution of social norms*, 7 *Yale J. L. & Tech.* 1 (2004), 3: *"Code and law regulate our behavior in different ways; while the law typically regulates behavior after the fact, code or architecture regulates "more directly," as "present constraints." These differences are important, as a practical matter, to the "legal engineering" choice of how to regulate different kinds of activities".*

[155] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 301: "*Potential PBD legislation, in particular, also requires flexibility, since it is nearly impossible to delineate every design and technical requirement and also unhelpful to overly prescribe the PBD solutions. The goal indeed, therefore, is for the potential PBD legislation to be as broad and comprehensive as possible when mandating the implementation of PBD solutions. Nevertheless, the PBD solutions will also need to consider the specific characteristics and privacy threats/risks of the different devices, systems or technologies concerned".*

[156] KIANIEFF, *The evolution of consumer privacy law: how privacy by design can benefit from insights in commercial law and standardization*, cit., 28: "*The words of Warren and Brandeis are particularly appropriate today since they emphasize that in order to safeguard this right, the law must adapt and keep pace with technology. Otherwise, a further erosion of privacy rights will occur as old problems creep up in new forms. If this fate is to be avoided, the law must remain vigilant to ensure that technology develops in a manner that enhances and does not hinder individual liberty".*

informazioni, spesso di terze persone, che non si volevano davvero pubblicare e che sarà più tutelato anche secondo un'ottica relazionale[157]. L'utente, che si ribadisce essere al centro dell'approccio di privacy by design, sarebbe più responsabilizzato e maggiormente consapevole di ciò che accade nella Rete perché sarebbero chiare le scelte e le possibilità per gestire la riservatezza. L'idea è di diminuire quell'asimmetria informativa di cui si è scritto attraverso la predisposizione di criteri di usabilità del sistema che rendano l'individuo consapevole, abile e un soggetto attivo, che può costruirsi da sé una tutela adatta alla sua aspirazione di riservatezza[158]. Si potrebbe persino mirare ad una situazione in cui i dati già divulgati diventino inaccessibili e così le informazioni introvabili o quantomeno sia molto più difficile poterlo fare, tutto grazie al design della tecnologia[159].

Concludendo, attraverso la privacy by design non si aspira solo ad una maggiore sicurezza nella circolazione dei dati personali, ma altresì ad un approccio globale. La tutela ex ante ha il pregio di minimizzare il rischio di verificarsi di violazioni della riservatezza degli individui e di infondere fiducia nei consumatori. Contemporaneamente, si ottiene la responsabilizzazione del soggetto privato, il quale incorpora la tutela della privacy all'interno dei propri prodotti[160]. Non solo, con uno sguardo più ampio, si può notare che due ordinamenti molto diversi tra di loro, ossia quello europeo e quello statunitense, hanno entrambi previsto questo approccio nel loro recente quadro normativo, dimostrando di potersi avvicinare in una materia come quella della privacy in cui hanno sempre optato per diverse soluzioni giuridiche. La stessa pbd assemblea degli elementi di ambedue gli ordinamenti: un forte ruolo affidato al soggetto privato e una flessibilità nell'adozione degli strumenti dovuta alla contemporanea presenza di obiettivi economici, che sono tipici dell'approccio tradizionale statunitense, e il robusto livello di tutela e di controllo da parte delle autorità, che contraddistinguono invece la posizione europea[161]. L'Europa inizia a tenere in maggior considerazione gli aspetti economici del costo di gestione dei dati e gli Stati Uniti allargano la tutela dei dati da sempre troppo settorializzata.

---

[157] Si veda PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 208.
[158] *Ibidem,* 210.
[159] Un'interessante riflessione sul concetto di "oscurità" dell'informazione grazie al design è contenuta in W. HARTZOG, F. D. STUTZMAN, *Obscurity by design*, 88 *Wash. L. Rev.* 385 (2013), 395: *"Instead, this Article proposes that general design principles to protect users of social technologies should be based on the concept of obscurity".*
[160] PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 200.
[161] *Ibidem*, 223.

5. Alcuni profili critici

Non si può a questo punto nascondere che ad oggi l'approccio di pbd non ha ancora trovato una diffusione capillare, a causa delle difficoltà nel definirlo in concreto e degli ingenti vantaggi economici ottenuti dalle imprese tramite il trattamento dei dati personali[162]. Inserire la privacy nel design è una questione critica, pur essendo un'iniziativa regolatoria estremamente importante[163].

C'è chi teme innanzitutto che la pbd indebolisca la privacy focalizzandosi molto sulla prevenzione e meno sul controllo della raccolta e spingendo troppo sull'implementazione di misure organizzative: il principio non si dovrebbe configurare come uno strumento volto esclusivamente alla promozione di forme di autoregolamentazione, ma più che altro dovrebbe mirare alla realizzazione di tecnologie protettive della riservatezza e alla responsabilizzazione dell'utente, il quale può scegliere il livello di protezione adeguato alle sue esigenze[164]. A questo proposito si ritiene di aver dato adeguato peso all'importanza dell'architettura privacy-friendly.

Nonostante si siano elencati nelle pagine precedenti molti vantaggi nell'assunzione del principio deve quindi essere dato conto di alcuni profili critici.

In primo luogo è stato evidenziato che la regola giuridica e la regola tecnica sono profondamente differenti perché la prima è caratterizzata da un procedimento formativo democratico, pubblico e garantista; mentre la seconda sarebbe carente del criterio di pubblicità nella creazione della norma perché è posta in essere dal tecnico nella costruzione della tecnologia e in quanto tale non né visibile e né trasparente. Le regole giuridiche per l'appunto sono presentate pubblicamente e malgrado la gran parte del processo legislativo si svolga a porte chiuse la legge è sempre pubblicata e disponibile potenzialmente a tutti e la sua applicazione è un'attività umana trasparente[165]. Al contrario, la

---

[162] *Ibidem,* 201.

[163] Sono molto dure e critiche le parole degli autori in MULLIGAN, KING, *Bridging the gap between privacy and design*, cit., 1033: *"Privacy by design is an exceedingly important regulatory initiative. Artifacts matter and ought to assist in protecting social values including privacy. However, building the right "privacy" into design is critical, and today regulators are working with an extremely cramped definition of privacy. Individual control may be the touchstone of data protection, but it is not the touchstone of privacy protection."*

[164] Si veda la critica in PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 225-226.

[165] TIEN, *Architectural Regulation and the evolution of social norms*, cit., 9: *"For the most part, legal rules are publicly created and presented. We should not overstate the degree to which the process of rule-creation really is public, of course. Much legislative activity takes place behind closed doors in the realm of lobbying, arm-twisting, and influence-peddling. Administrative regulation in federal agencies is also public – but again with a significant back-room component. Nevertheless, the ultimate outputs – the rules themselves – are generally published and available, theoretically, to everyone. Rules, moreover, need some minimal level of enforcement to be meaningful. Enforcement of rules is normally a complex, enterprising human activity".*

regolazione tramite la tecnologia implica minor trasparenza e l'esecuzione non spetta più all'uomo, ma alla macchina, con la conseguente perdita del conflitto sociale contro le norme[166]. In merito si è scritto provocatoriamente che i programmatori e gli ingegneri potrebbero diventare i legislatori del ventunesimo secolo, agendo su richiesta delle società commerciali e dei governi[167]. A tutto ciò si replica che la privacy by design non intende prendere il posto del diritto; piuttosto ambisce a diventarne strumento applicativo, perché il codice non è un sostituto, ma un suo è complemento[168]. Ancora una volta si ribadisce che è onere del diritto selezionare i limiti e i poteri del principio in questione. D'altro canto, non si può pensare che la pbd sia applicabile in ogni contesto: l'approccio è globale, ma non totalizzante.

Si è poi criticato il concetto perché condurrebbe ad una forma di controllo sociale, dal momento che l'architettura tecnologica modella le pratiche sociali in modo diretto, consentendo o negando le azioni senza garantire la possibilità di scelta[169]. Da ciò consegue che socialmente non si percepisca come regola ciò che appare già come una condizione del reale, non potendo decidere se obbedire o meno ad una prescrizione[170]. In realtà la privacy by design non intende limitare la libertà degli individui, ma mira a potenziarla e garantirla nelle situazioni in cui potrebbe essere fortemente minacciata con il controllo e lo sfruttamento delle loro informazioni personali.

Un punto di criticità può essere sollevato se si considera la diffusa ignoranza o scarsa conoscenza sociale in materia tecnologica; infatti, la persona comune non saprebbe capire se un sistema sia progettato correttamente o se avrebbe dovuto essere differente e ciò farebbe sfumare le potenzialità e gli incentivi nel potenziare le garanzie per ottenere la fiducia del

---

166 *Ibidem,* 10: *"From the enforcement perspective, then, architectural regulation bypasses many of the possibilities for human actors to modulate the effects or meaning of a rule in the enforcement process. Enforcement is instead delegated to equipment or social settings, lessening the possibility of social contest over the rule. The ordinarily public process of social conflict over rules may be short-circuited simply because we do not see what is happening".*

167 KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 283: *"Code as law may arguably be one way of bypassing regular democratic procedures of lawmaking and/or law enforcement to regulate or restrict human behavior and activities. Computer programmers/engineers, in this sense, could theoretically become the new lawmakers of the 21st Century, acting at the request of either corporations or governments".*

168 *Ibidem,* 299: *"PBD solutions and computer code are not a substitute or replacement for law, but rather are complementary".*

169 Si veda TIEN, *Architectural regulation and the evolution of social norms*, cit., 11.

170 *Ibidem,* 12: *"Architectural regulations are at the extreme perceived more as conditions than as rules to be followed or disobeyed consciously. Unlike ordinary sanction-backed rules, architecture achieves compliance by default rather than through active enforcement. To the extent that legitimacy and public deliberation are integral to our notion of law, the surreptitious enactment and enforcement of norms via architecture should give us pause. As a result, we may not perceive architecture normatively, as something intended to control us, but rather as experienced background conditions that just happen to exist".*

consumatore, che appunto sarebbe privo degli strumenti adatti[171]. Una soluzione prospettabile per contrastare questo elemento di critica potrebbe essere una maggiore diffusione capillare delle campagne pubblicitarie e sociali sulla privacy, per aumentare la conoscenza generale e generare una sensibilità attenta anche nell'uomo comune.

Un ulteriore profilo critico è l'inevitabile imposizione di un limite all'innovazione tecnologica. Al di là delle questi di principio, è chiaro che soprattutto in questo campo si dovrà sempre compiere un bilanciamento tra diverse forme di libertà e tra differenti diritti. Tra l'altro, le tecnologie di pbd potrebbero essere di per sé innovative ed aumentare il progresso delle scienze[172].

Quando si considerano le problematicità dell'approccio si può ricordare che grazie alla pbd si crea un circolo virtuoso composto da una maggiore sensibilità sociale, un aumento del potere e della tutela giuridica del consumatore e un adeguamento delle imprese a standard più protettivi della privacy.

Un aspetto di notevole criticità, tuttavia, è la difficoltà nel tradurre le regole giuridiche in linguaggio tecnologico poiché le norme si compongono di enunciati linguistici complessi e soggetti ad interpretazione, arduamente decifrabili dal sistema binario degli elaboratori elettronici. La traduzione dalle norme scritte e dai principi giuridici alle soluzioni tecniche del codice è evidentemente una sfida[173]. Nondimeno, non mancano degli esempi di ricerche sul campo, che abbiano saputo coniugare le due diverse tipologie di linguaggi e abbiano dimostrato che il lavoro congiunto tra giuristi e tecnici può condurre a soluzioni più che spendibili nel concreto. Si intende far riferimento alla ricerca compiuta da Paolo Guarda e Nicola Zannone dell'Università degli Studi di Trento, i quali hanno contribuito a fornire gli strumenti per lo sviluppo dei *privacy-aware systems* e hanno dimostrato che esiste la possibilità di progettare tenendo conto delle regolamentazioni giuridiche, prendendo come punto di partenza la traduzione e l'esplicazione delle norme[174]. Un altro contributo critico sostiene

---

[171] In questo senso sull'ignoranza tecnologica si veda sempre TIEN, *Architectural regulation and the evolution of social norms*, cit., 18: "*This ignorance has normative implications. To say that a system is wrongly designed, or that it should have been designed differently, requires knowledge about design options and tradeoffs. If information about alternative design options does not reach the public, a basis for such normative judgments vanishes. But even if the public did perceive bad design, it might not perceive it as wrong design without knowledge that there was a decision to design it that way. Where equipment affects privacy, lack of knowledge is especially important because it is often difficult to detect privacy invasions".*

[172] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 317: "*Moreover, some PBD solutions or concepts could perhaps be innovative in themselves and could lead to further innovation in other related or even unrelated areas".*

[173] *Ibidem,* 283.

[174] Si veda P. GUARDA, N. ZANNONE, *Towards the development of privacy-aware systems,* 51 *Info. & Software Tech*. 337 (2009).

all'opposto che sia troppo oneroso tradurre le norme giuridiche per trasporle nei codici informatici, soprattutto perché le norme giuridiche sono generalmente formulate in modo tale da consentirne un'applicazione flessibile[175]. Le plurime interpretazioni richiedono perciò una conoscenza approfondita e uno studio minuzioso allo stadio del design e, anche se ciò fosse possibile, la compatibilità potrà essere dichiarata solo da una corte e sarà soggetta all'evoluzione e alla dinamicità tipica delle norme giuridiche[176]. A ciò si aggiunge che le fonti giuridiche sono plurime e derivanti da diversi ordinamenti giuridici; infatti se si analizza la disciplina della privacy applicabile in Italia, si dovrà considerare il Codice Privacy, la disciplina settoriale, i pareri del Garante, le Direttive e i Regolamenti europei, le linee guida internazionali e così via. Questa ricerca è molto complessa, anche per un giurista. Tuttavia lo stesso contributo appena citato, che è il più critico sull'approccio tra i vari papers analizzati, apre ad una possibilità per la pbd: gli sviluppatori dei sistemi e chi li commissiona dovranno internalizzare il quadro normativo grazie ad un lavoro congiunto con i giuristi ed imparare a tenere in seria considerazione la privacy sia al momento della progettazione sia in quello successivo del monitoraggio di ciò che è stato prodotto[177].

Se i tecnici non saranno coadiuvati nel loro lavoro di implementazione, potrebbero avere delle difficoltà nel comprendere il significato e la portata della privacy by design. In particolare, è stato notato che la formulazione dei sette principi di Ann Cavoukian sia assai fuorviante e poco concreta, legata più a slogan che a linee di azione sistematiche[178]. Anche le norme che prescrivono l'adozione della tutela della vita privata fin dalla progettazione potrebbero risultare oscure agli addetti ai lavori dal momento che non apparirebbero

---

[175] B. J. KOOPS, R. LEENES, *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*, 28 *Int. Rev. Law Comput. Tech*. 1 (2013), 6: "*Finally, and this is perhaps the main complicating issue, many legal requirements have been formulated in such a way as to allow flexible application in practice".*

[176] *Ibidem,* 6: *"Complying with legal rules that are open to interpretation requires taking into account relevant case-law, legal history, and other relevant sources for assessing the legal status. Even if these sources could be studied at the time of system design, in the end the only authoritative answer to the question whether or not certain behavior is legally compliant can only be given by the courts. Moreover, such an assessment is not only context-dependent but also dynamic, as interpretations of legal norms may shift over time. The idea of encoding legal norms at the start of information processing systems is at odds with the dynamic and fluid nature of many legal norms".*

[177] *Ibidem,* 8: "*A promising way forward for privacy by design is thus that the people who commission IT systems together with the system developers try and internalize the data protection framework as part of their mindset, and design the system on the basis of carefully considered privacy design strategies that work within the specific context of the system at issue. This may then lead to privacy design patterns, which involve various combinations of technical and organizational measures, including PETs. Privacy by Design would then mean to take privacy seriously in the design and operation of the system and designing procedures that monitor and maintain compliance once built".*

[178] Si veda SCHARTUM, *Making privacy by design operative*, cit., 157.

sufficientemente dettagliate o specifiche[179]. Un informatico ha affermato che la pbd sarebbe un tipico esempio di iniziativa legislativa che non fornisce una guida adeguata agli sviluppatori del software[180]. In ambito ingegneristico il significato del concetto non sarebbe chiaro perché la maggior parte dei principi includono il termine pbd nella spiegazione del principio stesso[181]. Ciò che sarebbe certo, invece, è che il principio di minimizzazione è al centro dell'applicazione della privacy by design: non tutti i dati sono necessari e studiare a fondo la situazione concreta consente all'ingegnere di approntare le soluzioni migliori. Attraverso due casi studio è stato dimostrato che la minimizzazione nella raccolta dei dati è attuabile tramite l'utilizzo di alcune tecniche di design sin dalla progettazione[182]. Vengono consigliati quattro passaggi: descrivere chiaramente le funzionalità del sistema, per ciascuna di essa minimizzare la raccolta di dati a quelli strettamente necessari, tenere conto delle esigenze di sicurezza e infine implementare la soluzione che soddisfa i requisiti di integrità dei dati mostrandone la minore quantità possibile[183].

---

[179] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 284.

[180] A. MASSEY, *Why understanding technology is essential for privacy law*, 51 *Idaho L. Rev.* 695 (2015), 697: *"Privacy by Design (PbD) is an excellent example of a policy initiative that does not provide enough specific guidance to be practical for software engineers".*

[181] S. GÜRSES, C. TRONCOSO, C. DIAZ, *Engineering privacy by design*, Conference on Computers Privacy Data Protection 317 (2011), 3: "*Despite its comprehensiveness, it is not clear from Cavoukian's document, what "privacy by design" actually is and how it should be translated into the engineering practice. Most of the principles include the term "privacy by design" in the explanation of the principle itself".*

[182] Nel contributo intitolato *Engineering privacy by design*, è presentato un caso di studio sul sistema di petizione online. I nomi e le firme dei soggetti che aderiscono all'iniziativa vengono generalmente raccolti in un database. Gli autori del paper propongono la creazione di un sistema di petizione anonimo, grazie alla tecnica della crittografia. Nel dettaglio si prevede l'utilizzo di credenziali anonime associate all'utilizzo di un'identità elettronica, verificata da un'autorità, ma generata dal sistema all'atto della registrazione in modo che l'autorità non sia in grado di risalire alla persona fisica. Dovrà poi essere utilizzata una rete di comunicazione che consente l'anonimato (come la navigazione in incognito) perché potrebbero residuare dei rischi per la protezione dei dati personali se non si usasse il *network* corretto. Per una presentazione completa del caso si vedano le pagine 11-13.

[183] *Ibidem,* 13: *"Functional Requirements Analysis: The first step in the design of a system with privacy embedded at the core is to clearly describe its functionality. That is, the goal has to be well defined and feasible. Data Minimization: For a given functionality, the data that is absolutely necessary to fulfill the functionality needs to be analyzed. Modelling Attackers, Threats and Risks. Multilateral Security Requirements Analysis: Besides the system's purpose itself, an engineer must account for other constraints that ensure the security and correct behavior of the entities in the system, as expected by the different stakeholders of the system. The inclusion, analysis and resolution of these convicting security requirements is also known as multilateral security. The objective of this analysis is to find a design in which privacy measures cannot be detrimental to other important security objectives such as integrity, availability, etc. and vice versa. Implementation and Testing of the Design: The final step in the design of the system is to implement the solution that fulfills the integrity requirements revealing the minimal amount of private data".*

Senz'altro il punto dolente del principio di privacy by design è il costo della sua applicazione. Un'azienda, infatti, è costretta a spendere ingenti risorse per progettare i sistemi, acquistarne i migliori e assumere personale qualificato. Il costo dei programmi più sicuri è inserito nella voce dei costi dei servizi e quello del personale ricopre una voce a sé nel bilancio. Minore sarà la dimensione dell'azienda, maggiore sarà l'impatto delle uscite dovute al rispetto della normativa.

Nel merito, le aziende oggigiorno ottengono ingenti vantaggi economici dallo sfruttamento dei dati personali. Alcuni economisti hanno analizzato la relazione tra costi e benefici e hanno osservato che la quantificazione delle perdite dovute alle violazioni di sicurezza e la probabilità che esse si verifichino giocano un ruolo fondamentale; queste informazioni comunque non sono difficilmente ottenibili, con la conseguenza che in loro assenza le aziende optino per delle analisi alternative alla valutazione dei costi-benefici, come l'approccio che prevede degli *incremental budget adjustments*, ossia degli aggiustamenti progressivi al tetto di spesa in base a dei fattori esterni, come le cause in materia di privacy[184]. La stessa dottrina economica insegna che un'azienda si preoccupa di privacy solo se ciò contribuisce alla crescita dei profitti grazie all'attrattiva di nuovi consumatori[185]. Nel paragrafo precedente si è detto che la pbd può contribuire ad un aumento di fiducia nel consumatore e condurre ad un beneficio per i soggetti commerciali. Se ciò non fosse sufficiente a superare la problematicità dei costi, si giungerebbe ad una situazione in cui le aziende sarebbero estremamente riluttanti nel destinare proprie risorse nell'implementare la pbd, pur consapevoli del rischio di essere dichiarate responsabili a livello giuridico per non aver adottato una normativa vincolante.

A parere di chi scrive, la criticità dei costi potrebbe essere ridotta dal loro inserimento nella voce delle immobilizzazioni: garantire al consumatore/cliente un trattamento dei dati personali più sicuro sarebbe una spesa di utilità pluriennale, rinviabile in più esercizi economici. Una volta progettato il sistema in modo adeguato e privacy-friendly, il costo sarà assunto in un'unica soluzione ma distribuito nel tempo. Un'ulteriore possibilità è la previsione di investimenti

---

[184] Come è riferito in RUBINSTEIN, *Regulating privacy by design*, cit., 1437: "*Economists who have analyzed how much firms should invest in information security generally agree on three points. The first is that cost-benefit analysis is a sound basis for decision making. Under this approach, firms must estimate both the costs and expected benefits of security activities, which in turn requires estimates of the potential losses from security breaches and the probability of such breaches occurring. The second is that firms are more likely to utilize cost-benefit analysis if there is reliable data to inform the analysis. Here, however, that data on potential losses and their probability is hard to come by. The third is that in the absence of such data, many firms rely on alternatives to cost-benefit approaches such as incremental budget adjustments (i.e., adjusting the prior year's budget up or down based on possibly extraneous factors) or a more reactive approach (i.e., increasing investments in response to a breach event that makes security a must-do project)".*

[185] *Ibidem,* 1438.

pubblici per le aziende; difatti i soggetti economici potrebbero beneficiare di fondi pubblici e così in un regime di ricerca aperta e non secretata, potrebbero scambiarsi le informazioni sulle migliori soluzioni attuabili[186].

Tra l'altro gli strumenti e le misure di privacy by design potrebbero dipendere dalle dimensioni e dalle possibilità del titolare del trattamento, considerando le varie esigenze economiche delle imprese[187]. Non si dimentichi che i costi di implementazione sono previsti nell'articolo 25 del GDPR e che quindi, almeno nel nostro ordinamento, si avrà una norma che ha già previsto un contemperamento degli interessi in gioco, ma che garantisce un *minimum* di tutela.

Concludendo, le violazioni della privacy sono dovute al comportamento umano, se la tecnologia impedisse la maggior parte di questi comportamenti, gli abusi potrebbero essere minimizzati e disincentivati. L'elaboratore è una macchina dalle potenzialità immense, ma davanti ad una tastiera c'è sempre un uomo che digita il comando da eseguire. La pbd non potrà operare per ogni trattamento di dati personali, ma la si può ritenere il futuro della loro protezione.

6. La prospettiva futura

In questo paragrafo si intendono delineare le linee guida da seguire per l'auspicabile adozione giuridica del principio di privacy by design.

Innanzitutto la norma dovrà essere chiara, vincolante e applicabile al maggior numero di situazioni possibili. All'uopo il legislatore provvederà a definire il principio con norme prima generali e poi settoriali, per esempio definendo concreti requisiti di adozione[188]. È suo compito assicurare che le prescrizioni siano sufficientemente chiare perché sono volte alla protezione del diritto fondamentale all'autodeterminazione e ad essere lasciati soli[189]. La normativa non dovrà essere statica, ma dinamica e dovrà essere aggiornata

[186] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 322: "C*ompanies, researchers and other stakeholders could also receive public funding to develop and validate a variety of PBD solutions, and then identify and exchange best practices and lessons learned for implementing PBD solutions, based on established facts/evidence and pilot demonstrations".*

[187] PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, cit., 215.

[188] Si veda SCHARTUM, *Making privacy by design operative*, cit., 159: *"Legislators aiming at facilitating privacy by design should thus specify as many conditions as they have confidence in, possibly on a rather detailed level, for instance by defining sub-conditions. […] Such regulations would imply concrete privacy by design requirements imposed by law".*

[189] D. KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* 4 *JIPITEC* 2190 (2013), 80: *"It is the regulator's mandate, however, to ensure that legislative requirements are sufficiently clear and that their adherence can be tracked (and enforced). Notwithstanding this obligation, the argument that any lack of clarity on the specific meanings of PbD in every context should mean that its legislative adoption should not be encouraged, cannot stand where the right sought to be protected is as fundamental as the right to informational self-determination and to be let alone".*

periodicamente; allo stesso modo l'implementazione nei sistemi dovrà essere monitorata regolarmente. La previsione di sanzioni è inevitabilmente necessaria, così come la neutralità tecnologica delle disposizioni.

Secondariamente, il catalogo dei soggetti obbligati dovrebbe comprendere, oltre ai titolari dei trattamenti dei dati, i tecnici sviluppatori dei sistemi ICT. Affinché la pbd sia operativa è importante coinvolgere i tecnici, le autorità di controllo, gli incaricati del trattamento e gli interessati[190]. A ciò si aggiunge che la cultura della privacy dovrebbe essere alla portata di tutti.

Inoltre, i tecnici dovrebbero essere edotti a seguire la metodologia già a partire dagli studi formativi. A constatarlo sono stati gli stessi ingegneri, i quali hanno sottolineato che la privacy by design richiede una competenza particolare, una conoscenza completa dello stato dell'arte della tecnologia e del quadro normativo di riferimento[191].

Le criticità prima illustrate possono essere risolte operando un bilanciamento tra i vari interessi in gioco. L'era digitale ha fatto assumere natura globale ai fatti e agli istituti giuridici. Ciò che si auspica è che l'elaborazione dottrinale possa condurre alla redazione di una norma sulla privacy by design applicabile al più alto numero di ordinamenti. Occorre allora incentivare la condivisione delle scelte operative in ambito interno e internazionale[192]. A vantaggio di questa visione vi è il profilo tecnologico, che può essere facilmente trasposto da un contesto all'altro. Si potrebbero sostenere le iniziative di *open innovation* e *open technology*[193].

Si è già espressa la necessità che la pbd sia percepita dai soggetti commerciali come un incentivo; in questo la politica può esercitare la propria influenza e i governi devono essere i primi ad attuarla. Il principio potrebbe essere inserito nei contratti e nelle licenze informatiche, all'interno delle condizioni sottoscritte dall'utente, per garantirne una maggiore applicazione e una responsabilità a livello contrattuale; oppure si potrebbe puntare all'introduzione esplicita nelle policies aziendali, magari associata ad una certificazione attribuita da un organismo esterno ed imparziale.

---

[190] *Ibidem,* 171: *"However, in my view it is important to invalidate a tacit limitation of privacy by design as something primarily being a responsibility and possibility for controllers. Instead, we should acknowledge that a system-by-design approach should also include information systems under the control of other related parties, in particular data protection authorities, processors and data subjects".*

[191] GÜRSES, TRONCOSO, DIAZ, *Engineering Privacy by Design*, cit., 20-21: *"From these experiences we derive that engineering privacy by design requires a specific type of expertise. This expertise is necessary to develop a privacy by design engineering practice. This includes the establishment of privacy engineering methodologies and the training of future experts who are informed about the state-of-the-art research in security and privacy technologies, legal frameworks and the current privacy and surveillance discourses".*

[192] MANTELERO, *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, cit., 686.

[193] Il carattere *"open"* contraddistingue quelle posizioni di pensiero che spingono verso una maggiore condivisione delle ricerche scientifiche a vantaggio di tutti.

Nelle pagine precedenti sono stati citati contributi dottrinali di giuristi, economisti, informatici ed ingegneri; ancora una volta si desidera ribadire la potenziale ricchezza insista nel lavoro che allacci più discipline. La pbd può servire per creare un ponte tra diverse figure professionali e per superare le separazioni tra gli attori commerciali unendo gli sforzi per la protezione della privacy[194].

A questo punto si procede con l'illustrazione di alcune metodologie generali per applicare il principio nel design dei sistemi informatici. Inizialmente si deve distinguere tra i processi *front-end e back-end*: un sistema si compone di funzionalità visibili all'utente, come gli strumenti per condividere i dati personali in un social network, e invisibili/nascoste, che sono quei processi che garantiscono la conformità al diritto, al regolamento interno all'azienda e alle preferenze espresse dal consumatore[195]. Poi, sono stati indicati cinque tranelli da evitare nel design dei prodotti informatici, divisi in understanding e action:

1. Il design non dovrebbe oscurare all'utente la natura e la quantità dei flussi di informazione potenziali, perché l'utente può utilizzare il sistema in modo informato solo se capisce le ripercussioni sulla sua privacy;

---

[194] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 323: *"If successful, PBD in the end could serve as a bridge between lawmakers, policy-makers, practitioners, engineers/designers and academics, and thus potentially evolve into a policy instrument for overcoming the separation of the variety of relevant stakeholders and actors, for minimizing the excessive division of their efforts to protect privacy and for identifying the concurrences, synergies and overlaps of their endeavors".*
Per l'importanza di coniugare le diverse professionalità si veda MASSEY, *Why understanding technology is essential for privacy law, cit.,* 710: *"Effective communication between engineers and policy makers must become commonplace to protect privacy and improve the state of technology policy. Engineers must seek to better understand and incorporate laws and regulations into the design of their technologies; this is not only an ethical imperative, but it is also a critical aspect of developing professional standards for software engineering. Policy makers and lawyers must seek to understand the technologies beyond a surface level. Far too often policy makers identify a general policy solution or principle and then fail to state it with enough specificity to be accessible to the engineers building tomorrow's technologies".* Ciò che risulta molto interessante è il fatto che l'incorporazione delle regole della *privacy* nella tecnologia non sia solo una questione di conformità alla normativa, o un imperativo etico, ma anche di rispetto di standard della professione ingegneristica. D'altra parte il panorama giuridico dovrebbe far sì che le norme e i principi siano più chiari e spendibili da parte dei tecnici.

[195] RUBINSTEIN, *Regulating privacy by design*, cit., 1422: *"Front-end activities are a design process for customer-facing products and services (i.e., those with which customers interact by downloading software, using a web service, and/or sharing personal data or creating user content). Back-end practices consist of data management processes that ensure that information systems (for both internal use and for sharing data with affiliates, partners, and suppliers) comply with privacy laws, company policies (including published privacy policies), and customers' own privacy preferences. Although distinctive, the two lifecycles overlap in that most products and services designed for the Internet combine a front-end component with back-end data handling".*

2. Il design non dovrebbe oscurare all'utente l'effettiva portata della divulgazione delle informazioni attraverso il sistema, permettendo all'utente di sapere quali e a chi sono condivise;
3. Il design non dovrebbe richiedere un'eccessiva configurazione all'utente per gestire la privacy, la quale deve essere una naturale conseguenza del normale utilizzo del sistema;
4. Il design non dovrebbe rinunciare ad un meccanismo esplicito e di massimo livello per fermare e riprendere la condivisione dei dati;
5. Il design non dovrebbe inibire gli utenti dal trasferire le pratiche sociali nelle tecnologie[196].

Probabilmente il più approfondito contributo in materia è stato prodotto dall'ENISA nel 2014 attraverso il Report intitolato *Privacy and Data Protection by Design, from policy to engineering*[197]. L'agenzia europea ha stabilito un insieme di linee guida tenendo conto sia degli aspetti legali che di quelli ingegneristici. Per lavorare al livello dell'architettura i criteri chiave sono: la scelta del tipo di relazione di fiducia tra i portatori di interessi, la scelta del tipo di interazione con gli utenti, la considerazione dei limiti tecnici e la definizione dell'architettura stessa[198]. La pbd deve essere inserita in un processo di continuo adeguamento alla normativa e dunque l'ENISA ha indicato delle strategie data oriented, qui di seguito riportate:

1. Minimizzare, ossia restringere la quantità dei dati personali trattati al minor numero possibile. Concreti esempi di design sono gli strumenti che implementino l'anonimizzazione, l'utilizzo di pseudonimi e la selezione prima della raccolta.
2. Nascondere, ossia impedire la semplice e aperta visualizzazione dei dati personali e delle loro relazioni congiunte, per impedirne gli abusi. Alcune

---

[196] Si veda S. LEDERER ET AL., *Personal privacy through understanding and action: five pitfalls for designers*, 8 *Pers. & Ubiquitous Computing* 440 (2004). Il paper è interamente dedicato all'esplicazione dei cinque tranelli del design, di cui si riportano:
Understanding
1. Obscuring potential information flow. Designs should not obscure the nature and extent of a system's potential for disclosure. Users can make informed use of a system only when they understand the scope of its privacy implications.
2. Obscuring actual information flow. Designs should not conceal the actual disclosure of information through a system. Users should understand what information is being disclosed to whom.
Action
3. Emphasizing configuration over action. Designs should not require excessive configuration to manage privacy. They should enable users to practice privacy as a natural consequence of their normal engagement with the system.
4. Lacking coarse-grained control. Designs should not forgo an obvious, top-level mechanism for halting and resuming disclosure.
5. Inhibiting established practice. Designs should not inhibit users from transferring established social practice to emerging technologies.
[197] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Privacy and Data Protection by Design–from policy to engineering*, 2014, in Rete: <www.enisa.europa.eu>.
[198] *Ibidem,* 14.

esemplificazioni sono il crittaggio dei dati, l'insieme delle tecniche per nascondere il traffico delle informazioni e per scollegarle le une dalle altre.

3. Separare, ossia trattare i dati personali in modo distribuito, possibilmente in compartimenti separati, affinché non siano ricreabili dei profili completi degli interessati. Al momento non si conoscono degli esempi concreti che implementino questa strategia. Rimane perciò tra gli obiettivi dell'ENISA individuare delle eventuali tecniche innovative.
4. Aggregare, ossia trattare i dati personali al più alto livello di aggregazione e con il minor dettaglio possibile con il quale siano ancora utili, in modo da diminuire le informazioni sul singolo e lavorare sui gruppi. Le esemplificazioni sono: "*aggregation over time, dynamic location granularity, k-anonymity, differential privacy and other anonymization techniques*"[199].
5. Informare, ossia garantire la trasparenza nel trattamento dei dati personali. Delle possibili tecniche di design sono la piattaforma P3P, gli avvisi alle violazioni dei dati, la predisposizione di strumenti interattivi per la gestione delle informazioni.
6. Controllare, ossia l'interessato dovrebbe essere in grado di tenere sotto controllo il trattamento dei propri dati, anche attraverso la rappresentanza. Delle utili tecniche di design sono: "user centric identity management and end-to-end encryption support control"[200].
7. Far rispettare, ossia si dovrebbe porre in essere e applicare una *privacy policy* compatibile con i requisiti legali. Gli esempi sono il controllo all'accesso ai dati personali e delle regolamentazioni stringenti per la gestione interna degli stessi.
8. Infine, dimostrare, ossia richiedere al titolare del trattamento di provare la conformità con la privacy policy e ogni requisito legale applicabile. Concretamente si richiede un sistema adeguato di gestione organizzativa, e l'utilizzo delle tecniche di logging e auditing[201].

Queste strategie, a parere dell'Agenzia, devono essere promosse dai legislatori perché la privacy by design non può essere semplicemente adottata dagli sviluppatori dei sistemi ICT e dai titolari del trattamento dei dati; in ogni caso, dovranno essere previsti degli incentivi e dei modelli successivamente adottati dagli stessi soggetti pubblici, con l'azione diretta delle agenzie degli Stati Membri[202]. L'ENISA suggerisce anche una revisione delle policies per

[199] *Ibidem,* 19.
[200] *Ibidem,* 21.
[201] *Ibidem,* 19 e ss. Tutte le strategie elencate sono state tradotte e sistematizzate dalle pagine centrali del Report.
[202] *Ibidem,* 50: *"In today's information and communication technology landscape, privacy by design usually does not happen by itself, but it needs to be promoted. Policy makers need to support the development of new incentive mechanisms and need to promote them. System*

evitare delle facili scappatoie: se il prodotto o il servizio non soddisfano il paradigma della privacy by design, non potranno essere conformi alla legge; affinché tutto ciò sia attuabile, le autorità preposte alla protezione dei dati personali e dei consumatori dovrebbero disporre dei poteri necessari per cercare ed occuparsi attivamente delle violazioni[203]. L'approccio multidisciplinare è prerogativa di questa agenzia ed è altrettanto consigliato per lo sviluppo della privacy engineering[204]. Tale branca dell'ingegneria dovrebbe fornire gli strumenti per un'intuitiva implementazione della privacy, facendo sì che tutto risulti più semplice[205]. È infine chiaro che la pbd debba essere promossa dai legislatori e inserita nelle loro normative[206].

In queste pagine si è cercato di dimostrare che la privacy by design è l'approccio del futuro della protezione dei dati personali e della riservatezza. La pbd è probabilmente la migliore opzione oggi presente per bilanciare il potenziale trade-off tra privacy e libertà da un lato e la sicurezza pubblica, commercio, dall'altro[207].

7. Un approccio comune al DRM?

Come si è accennato nel primo capitolo della presente tesi, l'incorporazione della regola nella tecnologia è una metodologia non completamente nuova nel mondo del diritto ed è stata largamente utilizzata negli ultimi decenni per proteggere i diritti di proprietà intellettuale, o per meglio dire, per garantire che i contenuti digitali coperti dal diritto d'autore e dagli altri diritti di privativa non subiscano delle pesanti violazioni, spesso dovute all'inevitabile dinamica generalizzata di condivisione e di pirateria createsi con l'era digitale.

A questo fine, sono stati elaborati diversi strumenti tecnologici, più o meno efficaci, che sono complessivamente raccolti nella dicitura DRM, ossia Digital

---

developers and service providers need clear incentives to apply privacy by design methods and offer privacy-friendly and legally compliant products and services. Public services must serve as a role model by increasing the demand of privacy by design solutions. Funding agencies of member states or the EU should require a successful privacy and data protection assessment of each project and planned or achieved results".

[203] *Ibidem,* 50: *"A revision of policy is necessary to eliminate loopholes. In particular, legal compliance of a product or service should not be possible if it is not designed under the privacy by design paradigm. Furthermore, data protection authorities should be equipped with extended mandates and funds to be able to actively search for data protection violations".*

[204] *Ibidem,* 51: *"The research community needs to further investigate in privacy engineering, especially with a multidisciplinary approach. This process should be supported by research funding agencies. The results of research need to be promoted by policy makers and media".*

[205] *Ibidem,* 52: *"Providers of software development tools and the research community need to provide tools that enable the intuitive implementation of privacy properties. Privacy engineering should become easier".*

[206] *Ibidem,* 53.

[207] KLITOU, *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, cit., 328.

Rights Management, e previsti da vari strumenti normativi in tutto il mondo[208]. DRM, dunque, sta ad indicare l'insieme dei sistemi tecnologici in grado di gestire, tutelare e accompagnare le regole di accesso e di utilizzo su contenuti digitali, tramite protezioni software o hardware[209].

In generale, sembra corretto affermare che l'idea sottostante alle tecnologie DRM sia equiparabile all'approccio di privacy by design, perché, appunto, fin dalla progettazione dei contenuti digitali si tende a prevenire le violazioni e limitare gli utilizzi abusivi, impedendo, ad esempio, la copiatura dei file o la loro riproduzione illimitata e indiscriminata. Tuttavia, non si può nascondere che le misure attuate nel campo del diritto d'autore non siano state sempre ben accolte dal panorama dottrinale, suscitando alcune perplessità[210]. Si auspica che la privacy by design, invece, malgrado le criticità già sollevate, si affermi e rimanga circondata da un contesto dottrinale per lo più favorevole, mirando ad essere uno strumento in più per la protezione dei dati personali.

Oltre ad una metodologia comune, si può sollevare una questione che coinvolge i DRM e ha a che vedere con la pbd. Se è vero che la presenza dei sistemi tecnologici DRM tutela dei diritti, e soprattutto il diritto d'autore, si nota che al contempo ne comprime degli altri e in particolare che causa delle grandi violazioni della privacy. Si spiega per l'appunto che un sistema DRM comporta l'acquisizione e il trattamento di dati personali perché dotato delle seguenti funzioni di base: "a) controllo sull'accesso al contenuto; b) controllo sugli usi del contenuto; c) identificazione del contenuto, dei titolari del contenuto e delle condizioni generali per l'utilizzo del contenuto; d) autenticazione dei dati di identificazione elencati al punto c)"[211]. Vengono così raccolti e trattati i dati degli utilizzatori, spesso con una modalità non rispettosa delle norme, tanto che è stato affermato persino che l'accostamento dei termini DRM e privacy ha richiamato la figura retorica dell'ossimoro[212].

Così, per evitare che un sistema posto a garanzia dei diritti finisca poi per violare altre regole giuridiche, si può pensare di introdurre, per quanto possibile, un approccio di privacy by design nei DRM, migliorando la tecnologia che

---

[208] Per un'approfondita trattazione sui DRM si veda R. CASO (a cura di), *Digital Rights Management - Il commercio delle informazioni digitali tra contratto e diritto d'autore,* Ristampa digitale, Trento, 2006.

[209] *Ibidem,* 5-6.

[210] F. CIUSA, I. VARGAS-CHAVES, *Considerazioni critiche nella dottrina giuridica italiana sul DRM*, in *Principia Iuris*, 2013, fasc. 1, 328: *"In relazione alla disciplina del diritto d'autore, si precisa allora che i DRM pongono almeno quattro differenti elementi di criticità: in tema di accesso all'opera, di libere utilizzazioni, di copia privata nonché del c.d. equo compenso".*

[211] CASO (a cura di), *Digital Rights Management*, cit., 100.

[212] A. PALMIERI, *DRM e disciplina europea della protezione dei dati personali* in R. Caso (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative: atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007,* Quaderni del dipartimento di Scienze Giuridiche, n. 70, Trento, 2008, 198.

coinvolge l'utilizzo di dati personali e così rendendoli privacy-friendly. Design all'interno del design, si potrebbe dire.

Questa possibilità è accreditata con un sufficiente grado di fattibilità da parte degli esperti, anche se mancano i necessari incentivi per il mercato di questi prodotti[213]. Le essenze delle regole a tutela dei dati personali dovranno in tal modo essere incorporate in DRM architettati per minimizzare l'uso di informazioni[214]. Dovrà a tal fine essere operato un bilanciamento tra la privacy e l'esigenza di controllo spettante ai titolari dei diritti sui contenuti digitali protetti dai DRM: la sfida sta nello sviluppare dei sistemi che preservino abbastanza garanzie da entrambe le parti[215]. Lo stesso autore appena citato ritiene che siano necessari degli incentivi per i soggetti coinvolti nella progettazione, in modo da passare dalle pagine degli articoli accademici alla realtà, la quale è contraddistinta dalle regole del mercato[216]. Sarà compito e responsabilità del diritto assicurare che la formulazione di standard tecnici dagli attori del mercato prenda in considerazione i valori della privacy[217].

D'altro canto anche il Gruppo ex articolo 29 in un *working document on data protection issues related to intellectual property rights* del 2005 ha notato che lo sviluppo delle tecnologie di digital rights management ha condotto oggigiorno ad un livello diffuso di tracciamento e di controllo degli utilizzatori dei prodotti[218]. L'autorità ha allora enfatizzato la necessità di preservare i dati degli utenti e di minimizzarne l'utilizzo, anche tramite la realizzazione di nuove tecnologie a loro protezione[219].

Si è appena evidenziato una possibile applicazione della privacy by design, i cui ulteriori risvolti concreti verranno approfonditi nel quarto capitolo, attraverso l'indicazione di alcune aree e contesti in cui è già stato impiegato il principio.

Nel capitolo che segue verranno per completezza presentate le esperienze canadesi e statunitensi in tema, per approfondire l'argomento in prospettiva

---

[213] *Ibidem,* 201.
[214] *Ibidem,* 211.
[215] J. E. COHEN, *DRM and Privacy,* 18 *Berkeley Tech. L.J.* 575 (2003), 611: *"Technically, then, the challenge lies in developing technical systems that preserve both enough privacy for users and enough control for rights owners".*
[216] *Ibidem,* 613: *"For privacy-regarding DRM technologies to move from the pages of academic articles into the drawing board and ultimately into the marketplace, those who participate in or underwrite real-world design processes need incentives to expand their frames of reference".*
[217] *Ibidem,* 613: "*Law's role in structuring DRM standard-setting processes is to ensure that the formulation of technical standards by market actors takes public values, including privacy values, into account".* In una pagina successive dello stesso contributo (617) si legge anche che: *"Law can fulfill its responsibility in its usual fashion, by defining individual rights and correlative obligations, but to do so effectively it must come to terms with both the inadequacy of "markets for privacy" and the central role played by DRM standards in defining rights and obligations as a practical matter".* Ancora una volta si avverte allora la necessità che il diritto esca dai suo schemi tradizionali e si apra alle nuove dinamiche con delle soluzioni innovative.
[218] Cfr. Article 29 Data Protection Working Party, *Working document on data protection issues related to intellectual property rights*, WP 104 05/EN.
[219] *Ibidem,* 5.

comparatistica ed evidenziare le norme che oggi richiamano la pbd oltreoceano, essendosi concentrati al momento prevalentemente sull’articolo 25 del GDPR.

Capitolo 3: La privacy by design in prospettiva comparata

"L'accostamento di una regola a quella che ad essa corrisponde in un altro ordinamento, nonché la constatazione empirica della loro concordanza o diversità, è verosimilmente tanto antica quanto lo è la presa di coscienza del dato giuridico"
Sacco, Introduzione al diritto comparato, 2011.

1. L'ottica comparatistica

In questo capitolo si analizzerà la presenza del principio di privacy by design nell'ordinamento statunitense e in quello canadese.

Si è scelto di approfondire il modello di tutela fornito negli Stati Uniti perché è in questo contesto che è stata elaborata la prima proposta di legge sulla pbd e che è stata garantita una sua applicazione concreta grazie all'attività della Federal Trade Commission; verrà, infatti, analizzato il Commercial Privacy Bill of Rights Act del 2011 e saranno riportati alcuni casi giurisprudenziali in cui la FTC ha imposto l'applicazione di misure attuative della pbd, malgrado l'assenza di una norma vincolante in materia. Tra l'altro non si può nascondere che la disciplina statunitense è di fondamentale importanza per una efficace protezione dei dati personali a livello globale, vista la presenza nei vari stati delle società leader nel settore dell'informazione e dei social media.

Il Canada, d'altro canto, è la terra madre di Ann Cavoukian e così il territorio che ha visto nascere il concetto di privacy by design. Questo ordinamento si pone a metà tra l'Unione Europea e gli Stati Uniti e non è ancora dotato di una norma disciplinante la pbd. È interessante esaminare l'interpretazione fornita su alcuni principi della privacy, presenti a livello federale, dall'Office of the Privacy Commissioner of Canada, per comprendere come la privacy by design possa essere introdotta in un ordinamento in forza dell'attività interpretativa pragmatica di un'autorità garante.

Infine verrà proposto un prototipo di norma sulla privacy by design, frutto di un'elaborazione congiunta tra Ann Cavoukian, in qualità di Information Privacy Commissioner dell'Ontario e dal Pamela Jones Harbour, Former Federal Trade Commissioner, per fornire un parametro di confronto con l'articolo 25 del GDPR e uno modello per l'auspicabile introduzione legislativa della pbd nei due ordinamenti d'oltreoceano.

2. Il modello statunitense

La disciplina statunitense della privacy, si è detto, è molto frammentata. Essa può essere suddivisa in due parti, di cui la prima concerne i principi, le disposizioni e gli emendamenti alla Costituzione, così come interpretati dalla giurisprudenza, e la seconda riguarda l'insieme di statutes e delle regolazioni di common law di diritto ordinario[1]. Entrambe le tipologie di formanti hanno contribuito a creare un sistema di tutela molto complesso, che si snoda tra il livello federale e quello statale, accomunati dal fatto che le regole hanno cercato di far fronte alle sfide delle nuove tecnologie, da un lato, e alla sicurezza nazionale, dall'altro.

La privacy law negli Stati Uniti è anche molto settoriale: ogni norma regola un differente ambito commerciale e un particolare contesto in cui il diritto è tenuto a garantire la libertà dei cittadini. L'ordinamento statunitense dunque non tutela i dati personali e la riservatezza con un approccio onnicomprensivo, su modello europeo, ma in modo settoriale e con un "miscuglio" di diversi gradi di protezione[2].

La tutela della riservatezza coinvolge più soggetti, con caratteristiche e ruoli diversi[3]. Come si è accennato, la Federal Trade Commission ha assunto da qualche anno un ruolo regolatorio in materia di privacy che va ben oltre alla vigilanza a cui è preposta. Il sistema di organizzazione federale, infatti, non ha previsto un organismo indipendente dedicato esclusivamente alla protezione della privacy o alle problematiche di regolamentazione di Internet[4]. La protezione dei cittadini statunitensi, visto il carattere economico dell'agenzia, è diventata così la protezione dei consumatori[5].

Il rischio che si corre è la svalutazione dei diritti fondamentali dell'individuo, a favore della prevalenza degli aspetti commerciali o di interessi aziendalistici[6]. Eppure, è proprio grazie ai lavori della FTC che le regole statunitensi sulla privacy vengono interpretate e poi applicate dalle società

---

[1] PAGALLO, *La tutela della privacy negli Stai Uniti d'America e in Europa, modelli giuridici a confronto,* cit., 69.

[2] SOLOVE, HARTZOG, *The FTC and the new common law of privacy*, cit., 587: "*Privacy law in the United States has developed in a fragmented fashion and is currently a hodgepodge of various constitutional protections, federal and state statutes, torts, regulatory rules, and treaties. Unlike the privacy laws of many industrialized nations, which protect all personal data in an omnibus fashion, privacy law in the United States is sectoral, with different laws regulating different industries and economic sectors*".

[3] N. LUGARESI, *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffré, Milano, 2000, 79. In questo testo si delineano i soggetti coinvolti, tra i quali spiccano i pubblici poteri, che agiscono con vari organismi e su vari livelli. Tra tutti si ricordano il Congresso, il Governo e le Agenzie Amministrative. L'ambito della sicurezza pubblica ha una grande importanza nell'ordinamento statunitense, soprattutto a causa del terrorismo.

[4] *Ibidem,* 102.

[5] *Ibidem,* 103.

[6] *Ibidem,* 104.

commerciali; di fatto, oggi l'agenzia assume il ruolo di autorità federale garante[7]. È stato appunto affermato che la regolazione della FTC è la più ampia e probabilmente la più importante componente del "privacy regulatory system" degli Stati Uniti[8].

La determinazione delle pratiche commerciali corrette e non dannose per la privacy dei consumatori statunitensi è contenuta nei vari Report e negli ordini a carattere inibitorio disposti nei procedimenti contenziosi promossi dall'agenzia. A questa documentazione si aggiungono una serie di guidelines, white paper e workshops, materiali questi proposti come chiari criteri guida per il commercio, ma che in realtà hanno un proprio peso regolatorio, come si è già argomentato[9].

Per quanto concerne la definizione della privacy by design, si è detto, è stato fondamentale il Report del 2012 intitolato *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymaker*, che sintetizza l'approccio corrente e futuro dell'agenzia in ambito di privacy: centralità alla pbd, scelte semplificate per le aziende e maggiore trasparenza[10].

Tuttavia, il dibattito statunitense per introdurre la pbd a livello legislativo è precedente; esso ha riguardato specialmente la previsione di misure organizzative per le aziende e in misura minore l'implementazione di soluzioni per proteggere la privacy già a partire dalla tecnologia[11].

Nel dicembre del 2011 i senatori John Kerry e John McCain hanno presentato al Congresso il Commercial Privacy Bill of Rights Act, un testo legislativo federale che intendeva imporre alle società commerciali l'implementazione di un approccio di privacy by design nello sviluppo dei loro

---

[7] SOLOVE, HARTZOG, *The FTC and the new common law of privacy*, cit., 600: "*Today, the FTC is viewed as the de facto federal data protection authority*".

[8] *Ibidem,* 588: "*The FTC reigns over more territory than any other agency that deals with privacy. Because so many companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation. FTC regulation is thus the largest and arguably the most important component of the U.S. privacy regulatory system*".

[9] *Ibidem,* 626: "*In addition to settlement agreements, the FTC has created a form of "soft law" that consists of guidelines, press releases, workshops, and white papers. […] These materials are purportedly offered by the FTC as guides, yet the FTC has never clearly articulated which parts of its recommendations are mandatory and which parts are simply best practices. Many have criticized this lack of clarity because they feel compelled to be overly cautious to avoid running afoul of opaquely defined boundaries. Nevertheless, because these materials serve to illuminate the FTC's philosophy and approach, as well as its interpretation of Section 5, these materials have weight. They may not be exactly akin to advisory opinions, but they can come quite close. Companies take the guidance in these materials seriously. In some cases, statements in these materials can become almost like rules*".

[10] *Ibidem,* 626.

[11] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 4: "*In the United States, the debate surrounding PbD as a mandatory part of a legislative framework centres around organizational obligations, rather than embedded technological solutions to protect privacy by default, such as PETs*".

prodotti e nella relazione con i propri consumatori; si presentava come la prima introduzione esplicita della pbd in un progetto di legge[12].

Il Commercial Privacy Bill of Rights Act ha riscosso sia elogi che critiche, ma è la prima vera e propria previsione legislativa di pbd in Nord America[13]. Malgrado non sia stato approvato dal Congresso e rimanga quindi una mera proposta senza seguito, è interessante notare come il testo abbia fornito gli spunti per i lavori della FTC in materia, in relazione soprattutto alla previsione di misure organizzative per le società.

Lo scopo dichiarato del progetto di legge era di stabilire un framework per la completa protezione dei dati personali degli individui sotto l'egida della FTC[14]. Nella sezione 103 rubricata proprio "privacy by design", si stabilisce che ogni soggetto commerciale destinatario del framework debba adottare un programma di information privacy onnicomprensivo, in proporzione alla mole, alla tipologia e alla natura delle informazioni raccolte, attraverso due azioni[15]. Si richiede alle società di implementare il programma durante tutto il ciclo di vita del prodotto mediante la sua incorporazione nei necessari processi di sviluppo e nelle pratiche commerciali; questi processi e queste pratiche devono essere

---

[12] A. CAVOUKIAN (a cura di), *Privacy by design, from rhetoric to reality,* Information & Privacy Commissioner, Ontario, Canada, 2011, available at: <www.privacybydesign.ca>, 184: "*In the U.S., omnibus privacy legislation does not exist, though it has been hotly debated for several years. Without getting into the pros and cons of such legislation, it is clear that omnibus legislation would provide a solid vehicle for enshrining the principles of Privacy by Design. There is already movement in this direction: in 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights that would require businesses that collect, use, store or transfer consumer information to implement a Privacy by Design approach when developing products and provide consumers with choices about how data are used, collected and shared. This is the first time that Privacy by Design has been explicitly included in a bill*".

[13] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 10: "*The Bill has received both praise and criticism, but notwithstanding this early controversy, it is so far the first piece of legislation in North America to include mention of 'privacy by design' as part of a mandatory privacy framework. Although it has recently stalled somewhat, the advent of the new EU Proposal may see a rejuvenated debate surrounding this Bill*".

[14] The Commercial Privacy Bill of Rights Act of 2011, available at: <https://www.congress.gov/bill/112th-congress/senate-bill/799/text>: "*To establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission, and for other purposes*".

[15] Sec. 103, Commercial Privacy Bill of Rights Bill of 2011: "*Each covered entity shall, in a manner proportional to the size, type, and nature of the covered information that it collects, implement a comprehensive information privacy program by:*
(1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on: (A) the reasonable expectations of such individuals regarding privacy; and (B) the relevant threats that need to be guarded against in meeting those expectations; and
(2) maintaining appropriate management processes and practices throughout the data life cycle that are designed to ensure that information systems comply with: (A) the provisions of this Act; (B) the privacy policies of a covered entity; and (C) the privacy preferences of individuals that are consistent with the consent choices and related mechanisms of individual participation as described in section 202".

progettate per tutelare l'informazione personale identificativa, la quale si basa sulle reasonable expectations di privacy degli individui e sulle rilevanti minacce, le quali devono essere protette[16].

Secondariamente, si prescrive alle organizzazioni di mantenere durante tutto il ciclo di vita dei dati una gestione appropriata dei processi e delle pratiche commerciali, che siano anche in questo caso progettati per assicurare che i sistemi informativi rispettino le disposizioni del framework, le privacy policies delle aziende e le preferenze degli individui riguardanti la natura del loro consenso e la loro partecipazione al trattamento dei dati[17].

Il Commercial Privacy Bill of Rights Act prevedeva poi che il suo enforcement spettasse alla FTC; per l'appunto, la violazione delle sue norme avrebbe dovuto essere considerata come un atto o una pratica *unfair* o *deceptive* ai sensi FTC Act[18].

La privacy by design contenuta nel progetto del 2011 era intesa come una progettazione di tipo organizzativo e una protezione necessariamente proattiva ed onnicomprensiva. Anche se la pbd non assumeva lo stesso significato oggi assegnatole in Europa, la sua esplicita menzione in un testo legislativo era volta ad aumentare la protezione dei dati personali già nello stadio di design dei processi e dei prodotti[19]. Inoltre, è interessante sottolineare che il programma di tutela della privacy così come previsto dal bill dovesse essere proporzionato alla quantità, alla tipologia e alla natura delle informazioni raccolte, ma non ai costi della sua implementazione. Perciò, l'adozione della pbd non avrebbe dovuto essere limitata da questioni economiche, come invece sembra essere ai sensi dell'articolo 25 del GDPR.

La proposta del 2011 è rimasta purtroppo lettera morta. È solo grazie all'apporto della FTC che la privacy by design viene oggi applicata in alcuni contesti nell'ordinamento statunitense, proprio sulla base dei criteri previsti dal Report citato e della possibilità di enforcement preannunciata dallo stesso bill.

[16] *Ibidem,* si veda sopra il punto (1).
[17] *Ibidem,* si veda sopra il punto (2).
[18] *Ibidem,* SEC. 402: "*Unfair or deceptive acts or practices. A knowing or repetitive violation of a provision of this Act or a regulation promulgated under this Act shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices*".
[19] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 11: "*Privacy by design in the US does not mean the same thing as that very same term does in the EU or Canada, as evidenced by the Kerry-McCain Bill and the language used by the FTC. What the US approach does accomplish, however, is that it specifically mentions PbD and provides a solid basis for increased personal data protection at the design stage of personal data processing systems and associated products*".

2.1 Tre casi di violazione della Sezione 5 del FTC Act

Un atto e una pratica sono considerati *unfair* o *deceptive* ai sensi della Sezione 5 del FTC Act se sono una rappresentazione materiale, un'omissione o un'azione che presumibilmente ingannano il consumatore e sono volte a suo svantaggio, ovvero se esse causano o potrebbero causargli un considerevole danno senza che questi lo possa ragionevolmente evitare, o che non sia controbilanciato dalla presenza di benefici per lo stesso consumatore o più in generale per la concorrenza[20]. Perciò, l'interpretazione del carattere di *unfairness* è molto importante perché segnala se un atto o una pratica commerciale sono considerati fonte di danno per il consumatore[21].

Quando la FTC ha ragione di credere che siano stati posti in essere atti o pratiche di tale natura, emette un reclamo verso il soggetto commerciale, esponendo le sue accuse[22]. Questo enforcement ha natura amministrativa e non giudiziaria. Il soggetto coinvolto può aderire al reclamo firmando un *consent agreement* e conformandosi alle richieste della Commissione, senza che ciò risulti un'ammissione di responsabilità; dopo una serie di passaggi formali, la controversia si può così concludere in via extragiudiziale.

Se, invece, il soggetto contesta le accuse dell'agenzia, si aprirà un processo speciale presso un giudice amministrativo, preposto alla verifica della meritevolezza delle accuse e della validità delle prescrizioni del reclamo. Concluso il processo a favore della FTC, il giudice confermerà l'order stabilito dalla Commissione, a cui possono essere allegate anche delle sanzioni amministrative, e il soggetto sarà tenuto ad adottare delle azioni conformate alle prescrizioni della FTC.

Sulla base di queste premesse, si intendono riportare tre casi di violazione del FTC Act in cui è presente il concetto di privacy by design.

---

[20] SOLOVE, HARTZOG, *The FTC and the new common law of privacy*, cit., 599: "*The primary source of authority for FTC privacy enforcement was Section 5, which prohibits "unfair or deceptive acts or practices in or affecting commerce." An "unfair or deceptive" act or practice is a material "representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment" or a practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition*. *Thus, in its enforcement under Section 5, the FTC had two bases for finding privacy violations "deceptive" trade practices and "unfair" trade practices*".

[21] C. J. HOOFNAGLE, *Federal Trade Commission Privacy Law and Policy*, UC Berkeley Public Law Research Paper No. 2800276, Cambridge University Press, 2016, available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800276>, 160: "*As a refresher, recall that an unfair practice is one that causes substantial consumer injury, the injury must not be outweighed by countervailing benefits to competition or consumers produced by the practice, and it must be an injury that could not have been reasonably avoided by the consumer. Unfairness matters are important because they signal when the FTC thinks substantial injury or harm has been caused*".

[22] Le informazioni sull'enforcement della FTC sono ricavabili in rete: <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

La prima controversia risale al 2011 ed è stata promossa contro la Frostwire, una società di sviluppo produttrice di un'applicazione per il file sharing sui sistemi Android. La FTC citò la compagnia perché il software prodotto condivideva i contenuti degli utenti di default e li caricava indiscriminatamente su Internet; in più gli utenti dell'applicazione avrebbero dovuto controllare separatamente ogni categoria di contenuto, come le foto o i video, per evitare l'upload automatico di tutti i file del dispositivo mobile e se, invece, desideravano condividerne uno avrebbero dovuto lasciar caricare tutti gli altri per poi deselezionare quelli non prescelti per lo sharing[23].

La Commissione ha disposto che le ingannevoli ed ostruzionistiche impostazioni di default comportano un "*unfair design*"[24]. Ciò ha giustificato un'azione legale nei confronti della società, ritenendosi violato il FTC Act per l'inconsapevole condivisione dei file conservati nei device dei consumatori[25].

Nel "*complaint for permanent injunction and other equitable relief*" del 7 ottobre 2011 la FTC ha lamentato che le impostazioni di default dell'applicazione non consentivano al consumatore di essere adeguatamente informato sulle conseguenze prodotte dalla sua installazione e che nemmeno un utilizzo precedente di un altro software poteva permettergli di essere consapevole[26].

---

[23] HOOFNAGLE, *Federal Trade Commission Privacy Law and Policy*, cit., 162: "*In the FTC's Frostwire case, the Agency sued a company in federal district court because it disseminated an application that was likely to cause users to unwittingly place their files on the internet. The application, by default on installation, marked many different kinds of files for sharing (all photos, all videos, etc.). The user had to uncheck each category to avoid sharing. Additionally, in order to share a single file, the user had to check a category box (such as videos) and then uncheck every video not to be shared on the network. The Agency characterized these user interface functions as "unfair design*."

[24] SOLOVE, HARTZOG, *The FTC and the new common law of privacy*, cit., 642: "*In FTC v. Frostwire, LLC, the FTC alleged that failure to notify users that many preexisting files on consumer computers would be designated for public sharing constituted an unfair design. Users who did not wish to share a large number of files had to go through the burdensome process of protecting the files one at a time by unchecking many prechecked boxes designating the files for sharing. The FTC noted that deceitful or obstructionist default settings constitute an unfair design feature*".

[25] Complaint for permanent injunction and other equitable relief, October 7 2011, *Federal Trade Commission v. Frostwire LLC and Angel Leon*, available at <https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon>, 1: "*The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a). As alleged herein, Defendants' FrostWire for Android mobile file-sharing application was likely to cause a significant number of consumers installing and running it to unwittingly share personal files stored on their mobile computing devices with the public. Moreover, in their FrostWire desktop file-sharing application, Defendants misrepresented that certain files consumers downloaded from a file-sharing network would not be shared from the consumers' computers with the public*".

[26] *Ibidem,* 13: "*The Defendants had configured the application's default settings so that, immediately upon installation and set-up, many pre-existing files on the mobile device were designated for sharing. […] These shared files thus were available to other people in the*

Tra l'altro il design dell'applicazione e le sue impostazioni predefinite non erano controbilanciati dalla presenza di benefici e vantaggi per il consumatore o per la concorrenza[27]. Perciò, ai sensi della Sezione 5 del FTC Act quando una pratica dannosa non comporta altri vantaggi per il consumatore o per la concorrenza, essa viola il diritto e legittima la Commissione ad agire.

L'agenzia ha sottolineato che modificare le impostazioni dell'applicazione per evitare la condivisione indiscriminata e automatica avrebbe richiesto alla società minor costi in termini di tempo e di spesa rispetto alla scelta iniziale della progettazione e alla conseguente controversia[28].

In breve, la FTC ha stabilito nel *complaint* che il software di *FrostWire* causava o poteva causare un danno sostanziale ai consumatori, non evitabile e non bilanciato da altri vantaggi; pertanto la società distribuiva un prodotto con un "*unfair design*" e poneva in essere una pratica ingiusta e lesiva della Sezione 5 del FTC Act[29].

In risposta fu adita una corte federale della Florida, la quale, dopo una serie di indagini, emise uno *stipulated final order for permanent injunction* contro la società e a favore della FTC[30]. Nell'order il giudice, tra le varie prescrizioni, ha stabilito i requisiti per le impostazioni di default e il design del prodotto affinché fosse garantita la protezione dei diritti degli utilizzatori e consumatori. Fu imposto al convenuto, ai dirigenti, a tutti i suoi dipendenti e ai soggetti che collaboravano con la società di evitare permanentemente di distribuire o consentire il download dell'applicazione con le impostazioni

---

consumer's immediate vicinity and throughout the world to download and share further. Nothing in the installation and set-up process, described below, adequately informed consumers of the immediate consequences of installing FrostWire for Android; nor could consumers be expected to know these consequences from any prior experience with other software".

[27] *Ibidem,* 17: "*Distribution of FrostWire for Android with the design and default settings described above provided few or no countervailing benefits to consumers or competition*".

[28] *Ibidem,* 17: "*Configuring software applications to allow the public disclosure of private files by default runs counter to standard software development guidance, and counter to established practices in the development of file-sharing applications. Changing FrostWire for Android so that no user originated files are shared by default upon completion of the application installation and set-up process, and so that consumers can affirmatively select the files they want to share, required relatively minor costs in programming time and expense*".

[29] *Ibidem,* 19-20: "*As described in Paragraphs 22-32, in numerous instances, Defendants distributed, or caused to be distributed, to consumers versions of the FrostWire for Android application that, when installed on consumers' mobile devices, caused or were likely to cause consumers to unwittingly publicly share files of multiple types already present on, or subsequently saved on, those devices, including consumers' pictures, videos, unprotected applications, documents, music and audio files, and ringtones. Defendants' actions caused or were likely to cause substantial injury to consumers that was not reasonably avoidable by consumers and that was not outweighed by countervailing benefits to consumers or competition. Therefore, Defendants' practices as described in Paragraph 41, above, constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n)*".

[30] United States District Court Southern District of Florida, *Federal Trade Commission v. Frostwire LLC and Angel Leon*, Case No. 11-23643-CV-GRAHAM, available at: < https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon>.

originarie[31]. Furono anche indicate le caratteristiche che la nuova applicazione avrebbe dovuto possedere per essere conforme al diritto e non danneggiare l'utente. Insomma, fu stabilito il corretto design del prodotto, conforme alla normativa e rispettoso dei diritti del consumatore.

Il caso *Frostwire* dimostra che un'autorità e una corte possono imporre ad un soggetto commerciale di applicare l'approccio di privacy by design per tutelare i diritti lesi da un sistema informatico. L'enforcement non è stato garantito grazie ad una norma riguardante la pbd in modo esplicito, ma si è utilizzato l'espediente dell'interpretazione estensiva del criterio di *unfair* per una pratica commerciale lesiva del diritto del consumatore.

Non è chiaro se la presenza di una norma esplicita sulla pbd nell'ordinamento statunitense, come elaborata ad esempio dal Commercial Privacy Bill of Rights Act, possa fornire uno strumento in più alla FTC o se la pbd sia già considerata rilevante nell'ordinamento in forza della sua interpretazione evolutiva. Ciò che sembra probabile è che una volta statuito un criterio da parte di giudice a favore dell'agenzia, la FTC possa utilizzarlo come precedente in altre occasioni e quindi inserire nelle sue ingiunzioni l'adozione della privacy by design[32].

Il secondo caso coinvolge un colosso della tecnologia informatica quale è Google. La società che ha fornito il motore di ricerca più utilizzato al mondo

---

[31] *Ibidem,* 7-8: "*Requirements relating to user-originated files and default settings. IT IS FURTHER ORDERED that Defendants, their officers, agents, servants, employees, and attorneys, and all other persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, whether acting directly or indirectly, are permanently restrained and enjoined from, or assisting others in, distributing, enabling the downloading or installation of, or causing to operate any file-sharing application in commerce that can share user-originated files, unless any such sharing can be enabled only after the application is completely installed and set up, and the application:*
A. clearly and prom inertly discloses to the consumer which user-originated files, if any, the consumer can choose to share using the application, and the audience with whom those files would be shared;
B. is set, by default, to require the consumer to affirmatively select the specific, individual Gles to be shared, and to confirm after clear and prominent disclosure that selected Gles will be shared;
C. enables consumers to change the default settings described in Subsection III.B, above, provided that the application does not prompt the consumer to change those default settings, and only if the consumer: 1. affinnatively selects an option to do so after clear and prominent disclosure about the effect of the change and confirms the change through an affirmative selection; 2. must affirmatively select any groups of files to be shared; 3. after making any change to a default setting described in Subsection lll.B, above, can re-enable the default setting immediately upon taking actions substantially equivalent to those required to change it;
D. allows the consumer to disable sharing of any files or groups of files immediately upon taking actions substantially equivalent to those required to select them for sharing; and
E. provides a clearly labeled link or distinctive icon linking from the application's listings of shared files to clear and prominent written, graphical, and audiovisual instructions about how to disable sharing of files".

[32] A. HASTY, *Treating consumer data like oil: how re-framing digital interactions might bolster the federal trade commission's new privacy framework*, 67 *Fed. Comm. L.J.* 293 (2014-2015), 323.

lanciò nel 2010 Google Buzz, uno strumento di social network e microblogging implementato nel servizio di posta elettronica Gmail. Ad oggi il servizio è stato ritirato proprio a causa delle accuse della FTC ed è stato sostituito dall'applicazione Google+, che è sempre un servizio di social networking[33]. All'epoca Google intendeva competere con Facebook inserendo nel web un nuovo social network che fosse interconnesso con tutte le sue varie piattaforme e con la mail dell'utente; per far ciò, la società caricò nei vari profili degli utenti utilizzatori di Gmail tutti i loro contatti di posta elettronica, rendendoli così pubblici[34]. È facilmente intuibile che questa pratica infuriò gli utenti ed attirò l'attenzione della FTC.

La Commissione allora emise un reclamo contro Google, ritenendo che fosse stata violata la Sezione 5 del FTC Act attraverso la *"falsely representing to users signing up for Gmail that it would use their information only for the purpose of providing them with web-based email"*[35]. Si lamentava a Google di aver ingannato il consumatore utilizzando le sue informazioni per un scopo eccedente a quello per il quale erano state raccolte, ossia la fornitura di un servizio di posta elettronica, di averlo raggirato impedendogli di rifiutare l'iscrizione a Google Buzz, di non avergli riferito in modo adeguato che certe informazioni sarebbero diventate di dominio pubblico per impostazione predefinita e infine di aver rappresentato scorrettamente la conformità con il U.S.-EU Safe Harbor Framework, meccanismo volto alla protezione dei trasferimenti di dati tra l'Unione Europea e gli Stati Uniti[36].

L'agenzia propose a Google un order nel quale indicava le prescrizioni da attuare per evitare di essere coinvolta in futuro in simili pratiche commerciali

---

[33] Per il ritiro di Google Buzz si veda: <https://support.google.com/mail/answer/1698228?hl=it>.

[34] C. J. HOOFNAGLE, *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) *IEEE Security & Privacy* 58 (2016), available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163>, 5: "*The FTC has pursued Google for several privacy deviations. The original matter concerned how the company deployed its social network Buzz. Google was eager to compete with Facebook in the social network market and needed to quickly populate its system so that users would peel away from Facebook and spend more time in the Google platform. Google did this by loading users' profiles automatically with their most frequent email contacts. However, in doing this, Google made these frequent email contacts public. Apparently, the company did not consider that users might have confidential or complex, contentious relationships with others that would become endangered through publicity*".

[35] Federal Trade Commission, Google, Inc.; *Analysis of proposed consent order to aid public comment*, 76 *Federal Register*, April 5 2011, available at <https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter>, 18763.

[36] *Ibidem,* 187663: "*The complaint also alleges that Google falsely represented to consumers that it would seek their consent before using their information for a purpose other than that for which it was collected. The complaint further alleges that Google deceived consumers about their ability to decline enrollment in certain features of Buzz. In addition, the complaint alleges that Google failed to disclose adequately that certain information would become public by default through the Buzz product. Finally, the complaint alleges that Google misrepresented its compliance with the U.S.-EU Safe Harbor Framework, a mechanism by which U.S. companies may transfer data from the European Union to the United States consistent with European law*".

scorrette[37]. Nel documento si ordinava a Google di stabilire, implementare e successivamente mantenere un comprehensive privacy program, ragionevolmente progettato per affrontare i rischi per la privacy dei consumatori connessi allo sviluppo e alla gestione dei nuovi prodotti e di quelli esistenti e per proteggere la privacy e la riservatezza delle informazioni tutelate[38].

Tale programma, il cui contenuto e la cui implementazione dovevano essere documentate per iscritto, doveva contenere dei controlli per la privacy e delle procedure appropriate in relazione alla dimensione dell'azienda del convenuto, alla natura e allo scopo delle sue attività commerciali e alla sensibilità delle informazioni raccolte, comprese la nomina di personale preposto alla sua attuazione, l'analisi dei rischi, l'elaborazione di nuove clausole contrattuali con gli internet service providers, il design e l'implementazione di misure organizzative e tecniche per la protezione della privacy, da monitorare costantemente e adeguare all'analisi dei rischi e alle risposte reali alla programmazione[39].

---

[37] *Ibidem,* 187663: "*The proposed order contains provisions designed to prevent Google from engaging in the future in practices similar to those alleged in the complaint with respect to all Google products and services, not only Gmail or Buzz*".

[38] Decision and order, Federal Trade Commission, Google Inc., DOCKET NO. C-4336 available at <https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter>, 4: "*IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information.*

[39] *Ibidem,* 4: "*Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information, including:*

A. the designation of an employee or employees to coordinate and be responsible for the privacy program.

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent's unauthorized collection, use, or disclosure of covered information, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of those privacy controls and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from respondent, and requiring service providers by contract to

implement and maintain appropriate privacy protections.

E. the evaluation and adjustment of respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program".

Google preferì aderire alle prescrizioni della Commissione e risolvere così la controversia in via extragiudiziale[40].

Nelle considerazioni della FTC è stata inserita l'adozione della privacy by design, concepita soprattutto come la predisposizione di misure organizzative a tutela preventiva dei diritti dei consumatori. Il riferimento esplicito ad un "comprehensive privacy program" comprova che il lavoro di proposta di legge dei due senatori statunitensi ha contribuito a sensibilizzare la FTC in materia di pbd. Si tratta della prima volta che la FTC inserisce tra le sue prescrizioni un programma così complesso sulla privacy e la prima occasione in cui utilizza il Safe Harbour come parametro per misurare le violazioni di una società[41]. Se si considera poi che Google ha ritirato il social network dopo le accuse della FTC, si comprende che il design di un prodotto o di un servizio è di vitale importanza per la sua conformità al diritto e perché no, al suo successo commerciale.

Infine, il terzo caso che si intende riportare è più recente e riguarda un operatore alberghiero, la Wyndham Hotels and Resorts. Nel 2015 a causa di alcuni problemi per la sicurezza dei dati, le carte di credito utilizzate dai clienti sono state hackerate e moltissimi consumatori sono stati danneggiati. La FTC ha ritenuto che la società violasse la Sezione 5 del FTC Act adottando delle pratiche scorrette e lesive della privacy dei consumatori.

Anche in questo contesto l'agenzia ha emesso un reclamo contro la società. Il giudice adito sul caso ha confermato le osservazioni della FTC decidendo per uno *stipulated order for injunction*, in cui si ordina di adottare un approccio di privacy e security by design. In particolare, è stato imposto alla Wyndham Hotels and Resorts di implementare un "comprehensive information security program" per la durata di vent'anni, progettato per proteggere la sicurezza, la riservatezza e l'integrità dei dati appartenenti ai titolari delle carte di credito, che sono dei consumatori[42]. Questo programma, di cui si richiede adeguata documentazione, deve consistere in misure amministrative, fisiche e tecniche, adatte alle caratteristiche del trattamento dei dati, tra le quali si inseriscono anche l'analisi dei rischi per la sicurezza e il design degli strumenti

[40] HOOFNAGLE, *Assessing the Federal Trade Commission's Privacy Assessments,* cit. 5.

[41] F. KHAN, *Survey of Recent FTC Privacy Developments and Enforcement,* 67 *Bus. Law.* 297 (2011), 301: "*For the first time, the FTC included an unexpected term by calling for the company to implement a "comprehensive privacy program to protect the privacy of consumers' information" to be assessed biennially by an independent professional. Also for the first time, the FTC charged a company with violating substantive privacy requirements of the US-EU Safe Harbor framework*".

[42] *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.,* Civil Action No. 13-1887 (ES), United States District Court for The District of New Jersey 2014 U.S. Dist. LEXIS 84913, available at: <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment>, 4: "*IT IS ORDERED that Hotels and Resorts shall, no later than the date of entry of this Order, establish and implement, and thereafter maintain, for twenty (20) years after entry of this Order, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Cardholder Data that it collects or receives in the United States from or about consumers*".

atti a prevenire le violazioni[43]. Ancora una volta si evidenzia l'importanza di un approccio preventivo per la tutela dei dati dei consumatori. L'imposizione di regole organizzative concrete può contribuire a rendere le attività commerciali conformi alla legge. In più nel caso Wyndham emerge la questione della necessaria sicurezza dei dati raccolti e trattati dai soggetti commerciali: non si deve aspirare solo alla privacy by design, ma anche e soprattutto alla security by design.

All'interno dell'ordinamento statunitense, grazie agli interventi e all'interpretazione della FTC, la privacy by design potrebbe rappresentare uno strumento atto a garantire una maggiore protezione dei diritti dei cittadini, in modo più coerente e completo. È vero che la Commissione si rivolge a contesti in cui i soggetti sono solo consumatori, ma ormai la dimensione economica coinvolge la maggior parte delle situazioni giuridicamente tutelabili e per le restanti soccorrono altre disposizioni, come il Quarto Emendamento alla Costituzione. In più, visto che le società coinvolte nelle indagini della FTC non operano solo nei confini statunitensi, ma a livello internazionale e anche in Europa, le imposizioni volte ad implementare la pbd potrebbero avere dei riflessi e degli sviluppi validi anche per altri individui in tutto il resto del mondo. A partire dal 2018 gli Stati Uniti dovranno fare i conti con il GDPR; allora si vedrà se i loro standard verranno ad essa adeguati o si dovrà trovare l'ennesimo compromesso per gestire e controllare quantomeno il trasferimento transfrontaliero dei dati europei.

3. Il modello canadese

Ad Ann Cavoukian si deve la prima elaborazione della privacy by design, attraverso i sette principi fondativi già descritti in precedenza, nel contesto

[43] *Ibidem*, 4: "*Such program, the content and implementation of which must be fully documented in writing, shall consist of the following administrative, technical, and physical safeguards appropriate to Hotels and Resorts' size and complexity, the nature and scope of Hotels and Resorts' activities, and the sensitivity of the Cardholder Data at issue:*
A. the designation of an employee or employees to coordinate and be accountable for the information security program;
B. the identification of material internal and external risks to the security, confidentiality, and integrity of Cardholder Data that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, (3) risks emanating from the Wyndham-branded Hotels, and (4) prevention, detection, and response to attacks, intrusions, or other systems failure;
C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment (including any risks emanating from the Wyndham-branded Hotels), and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures; […]".

canadese. Malgrado ciò, ad oggi nell'ordinamento canadese non è ancora presente una norma che codifichi esplicitamente il principio.

In Canada la privacy non è un diritto costituzionalmente garantito; essa viene tutelata grazie all'interpretazione della Sezione 8 del Charter of Rights and Freedom effettuata dalla Corte Suprema Canadese. Questa norma ha lo scopo di proteggere il cittadino dalle irragionevoli perquisizioni e sequestri da parte dello Stato, su modello del Quarto Emendamento alla Costituzione Americana[44]. La Corte nel caso Hunter v. Southam del 1984 ha stabilito, infatti, che il testo del Chapter garantisce un broad e general right ad essere al sicuro dalle irragionevoli intromissioni dello Stato, diritto che può essere esteso alla protezione contro le intrusioni alla privacy degli individui[45]. La Sezione 8, però, protegge la libertà del cittadino canadese solo nei confronti dello Stato e non la assicura dalle violazioni dei soggetti privati; perciò la protezione della riservatezza degli individui fornita dal Charter of Rights and Freedom è molto limitata[46].

Per quanto riguarda il rapporto tra privati il diritto alla privacy è protetto da una serie di legislazioni federali, provinciali e spesso settoriali, tra le quali emerge per importanza il Personal Information Protection and Electronic

---

[44] Charter of Rights and Freedom: Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11, available at <http://laws-lois.justice.gc.ca/eng/const/page-15.html#h-39>: "8. Everyone has the right to be secure against unreasonable search or seizure".
Si v. anche KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit, 3: "*In Canada, the right to privacy is not a constitutional right as such; rather, the constitutional right to privacy is rooted in and protected by the Supreme Court of Canada's interpretation of Section 8 of the Charter of Rights and Freedom, the right to be free from unreasonable search and seizure. This protection is similar to the right afforded by the American 4th Amendment, although one should not go too far in drawing parallels, as the jurisprudence in the US and Canada in this regard is certainly not uniform*".

[45] *Hunter v. Southam*, 2 S.C.R. 145, 159-60 (1984), par. 146 available at <http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5274/index.do>: "*The Canadian Charter of Rights and Freedoms is a purposive document, the provisions of which must be subjected to a purposive analysis. Section 8 of the Charter guarantees a broad and general right to be secure from unreasonable searches and seizures which extends at least so far as to protect the right of privacy from unjustified state intrusion. Its purpose requires that unjustified searches be prevented*".

[46] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit, 4: "*Section 8 protects the liberty of the person but only in so far as the individual has a 'reasonable expectation of privacy' in the conduct that is impacted by the intrusion or violation at the hands of the State, not applicable to intrusion by the private sector. Thus, constitutional protection of this privacy right is limited to where there is an infringement by the State of an individual's reasonable expectation of privacy. It is by no means an absolute constitutional right*".
Per i riferimenti alla PIPEDA si v. Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), disponibile in Rete: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>.

Documents Act (d'ora in avanti PIPEDA)[47]. In un certo senso, l'ordinamento canadese si pone a metà tra l'Unione Europea e gli Stati Uniti; esso tiene gran conto del problema dell'invasivo controllo sui cittadini compiuto dal Governo, che si comporta come un "grande fratello", ma allo stesso tempo si preoccupa di tutelare i diritti dei cittadini dagli abusi del settore privato, con un approccio più garantista, su modello europeo. La privacy canadese è intesa come il senso di controllo che permette agli individui di porre dei limiti sia al settore pubblico che a quello privato[48]. Ciò nonostante, in concreto il framework della privacy è frammentato, come accade nell'ordinamento statunitense.

La PIPEDA è una legge federale che si applica al trattamento dei dati personali effettuato dai soggetti commerciali quando non è presente una legislazione provinciale che disciplini il settore privato dell'informazione, ovvero quando il trattamento coinvolge territorialmente più province canadesi o il flusso delle informazioni è di carattere internazionale[49]. Il dato tutelato è quello che identifica un individuo, anche se non viene puntualmente definito nel testo legislativo[50]. La PIPEDA racchiude in sé sia l'esigenza di tutelare i diritti degli individui soggetti ad abusi, sia la presenza di interessi delle società commerciali, che hanno la necessità di utilizzare i dati e le informazioni a loro vantaggio economico; il risultato ottenuto è un framework completo e tecnologicamente neutrale[51].

---

[47] *Ibidem,* 4: "*Informational privacy rights in Canada are not constitutional rights. They are protected by private and public sector federal legislation such as PIPEDA and the Privacy Act, respectively, as well as by relevant provincial and sector-specific legislation*".

[48] A. LEVIN, M. J. NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 *U. Ottawa L. & Tech. J.* 357 (2005), 360: "*In Canada, we find that Canadians occupy the middle ground between the EU and the US, sharing American concerns about "Big Brother" government, while also having deep concerns about private sector abuse of their personal information. As a result, we find Canadians identify privacy with a sense of control that enables them as individuals to set limits upon both the public and the private sector*".

[49] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 7: "*PIPEDA is federal legislation and governs private sector organizations, while the Privacy Act governs the public sphere. The Provinces each have separate public sector legislation, but only four (Alberta, Saskatchewan, Manitoba and Ontario) have specific health-sector legislation. Essentially, PIPEDA applies to the processing of personal information relating to all commercial activities where there is no provincial private sector legislation, as well as to inter-provincial and international data flows, but it does not regulate activities related to the personal information of employees of provincially regulated organizations*."

[50] LEVIN, NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, cit., 379: "*The next significant step in protecting the personal privacy of Canadians was the passage of the Personal Information Protection and Electronic Documents Act (PIPEDA) in 1999. This legislation protects the privacy of personal information collected, used or disclosed in the private sector. It does not define personal information, however, except to the extent that it is information that identifies an individual*".

[51] A. CAVOUKIAN, P. JONES HARBOUR, *White paper for regulators, decision-makers, policy-makers*., in CAVOUKIAN (a cura di), *Privacy by design, From rhetoric to reality,* cit., 177: "*In Canada, as elsewhere, private sector privacy regulation recognizes the dual purposes of protecting the individual's right to privacy on the one hand, and recognizing the commercial need for access to personal information on the other. PIPEDA furthers these two purposes by*

Come si è accennato, non è presente in Canada una norma che preveda esplicitamente la pbd; eppure un'opinione dottrinale ritiene che si possano rilevare delle tracce di privacy by design nei principi del CSA Model Code for the Protection of Personal Information, a cui la legislazione canadese aderisce[52]. Nel 1996 la Canadian Standards Association (CSA) ha pubblicato uno statement costituito da un elenco di dieci principi sulla protezione dei dati dei consumatori definito il Model Code for the Protection of Personal Information, che rappresenta il primo standard nazionale e volontario per la protezione dei dati nello Stato[53]. Questo Model Code è stato elaborato sulla base delle linee guida dell'OECD del 1980 e, sebbene sia uno standard a cui aderire volontariamente, ha assunto nel tempo un'importanza sempre maggiore grazie alla sua larga applicazione all'interno delle società canadesi. Ad oggi, il CSA Model Code for the Protection of Personal Information costituisce una componente della PIPEDA e i suoi principi sono stati inclusi nella legislazione[54].

Il quarto principio del CSA Model Code statuisce che la raccolta di informazioni personali deve essere limitata a quanto è necessario per gli scopi identificati dall'organizzazione che le tratta; l'informazione poi deve essere raccolta mediante dei mezzi giusti e legali[55]. Il principio di minimizzazione può essere interpretato in modo estensivo per includere la privacy by design, così come si opera per il principio di necessità del Codice Privacy italiano, ma nel testo canadese non si fa accenno alla progettazione presente nel nostro articolo 3.

Piuttosto, la pbd può essere ricercata in un altro principio del Model Code, che prescrive delle safeguards da attuare durante il trattamento dei dati. Difatti, il settimo principio stabilisce che le informazioni personali degli individui

---

tying a set of flexible, technology-neutral privacy principles to a statutory framework of rules governing the collection, use, and disclosure of personal information".

[52] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 8: "*Neither PIPEDA nor any of the provincial equivalents contains an explicit PbD requirement. What the legislation does require is adherence to the privacy principles of the CSA Model Code for the Protection of Personal Information, which by implication may require data privacy considerations at the design stage of a system. A salient example of this would be Principle 4.7 regarding 'safeguards' (some of the suggested technological measures would need to be contemplated before bringing a system online) as well as Principle 4.4 regarding 'limiting collection'*".

[53] Si v. in Rete: <http://www.csagroup.org/legal/privacy/csa-group-privacy-statement/>.

[54] LEVIN, NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, cit., 380: "*PIPEDA has been modeled on the Canadian Standards Association (CSA)'s Model Code for the Protection of Personal Information which was developed by business and consumer groups as well as government and was established as a national standard in 1996. The Model Code contained ten privacy principles that have been included in the legislation*".

[55] Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, available at: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html>: "*4.4 Principle 4, Limiting Collection. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means*".

debbano essere protette attraverso delle misure di sicurezza adeguate alla sensibilità delle informazioni stesse[56]. Queste garanzie devono salvaguardare le informazioni dalla perdita e dal furto, così come dagli accessi, dalla divulgazione, dalla copia, dall'utilizzo o dalla loro modificazione, se non sono attività autorizzate, a prescindere dal formato in cui sono raccolte[57]. La natura delle tutele deve dipendere dalla sensibilità delle informazioni, dalla quantità, dalla distribuzione, dal formato delle stesse e dal loro metodo di conservazione[58]. Il metodo di protezione dovrà includere:

1. misure fisiche, come degli armadi chiusi o delle restrizioni all'accesso per i dipendenti;
2. misure organizzative, come delle autorizzazioni di sicurezza e accessi limitati;
3. misure tecnologiche, come l'utilizzo di password e di crittografia[59].

Infine, le organizzazioni devono rendere i propri dipendenti consapevoli dell'importanza della confidenzialità delle informazioni e utilizzare particolare attenzione all'eliminazione o alla distruzione delle informazioni personali per prevenire gli accessi indesiderati di terze parti[60].

In questo principio è possibile ritrovare una traccia implicita di privacy by design poiché si impone l'adozione di misure tecnologiche e organizzative, ma anche qui non si accenna alla progettazione dei prodotti e dei servizi. Leggendo più attentamente la disposizione però sembra essere chiaro il fatto che le misure di sicurezza debbano essere implementate fin da subito, dall'inizio della raccolta, essendo parametrate alla sensibilità delle informazioni, e per tutta la durata della conservazione, volendo prevenire ogni sorta di perdita e dispersione non autorizzata. La stessa formazione dei dipendenti dell'organizzazione è volta a sensibilizzarli sull'importanza della protezione dei dati e risulta un indice di una forte attenzione preventiva. La norma quindi

---

[56] *Ibidem*: "*4.7 Principle 7, Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information*".

[57] *Ibidem*: "*4.7.1: The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held*".

[58] *Ibidem*: "*4.7.2: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4*.".

[59] *Ibidem*: "*4.7.3 The methods of protection should include*
(a) physical measures, for example, locked filing cabinets and restricted access to offices;
(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and
(c) technological measures, for example, the use of passwords and encryption".

[60] *Ibidem*: "*4.7.4: Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. 4.7.5: Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3)*".

potrebbe essere interpretata estensivamente, in modo da introdurre il principio di pbd nell'ordinamento canadese, quantomeno a livello federale.

Non a caso l'interpretazione dei principi della PIPEDA compiuta in questi ultimi anni dalle autorità garanti della privacy, nell'ambito di alcuni procedimenti contro delle aziende, tende ad inserire nel quadro normativo canadese la pbd. Questo principio è considerato come il futuro della protezione della riservatezza e dei dati personali già a partire dalla riflessione dell'allora Commissaria della Provincia dell'Ontario Ann Cavoukian.

3.1 Alcuni casi di utilizzo della privacy by design da parte dell'Office of the Privacy Commissioner of Canada

A differenza degli Stati Uniti, in cui la FTC ha elaborato un Report sulla privacy by design, l'Office of the Privacy Commissioner of Canada (d'ora in avanti OPC), l'autorità federale preposta alla promozione e alla tutela della privacy, non ha emesso alcun parere dedicato alla tematica, ma ha espresso più volte la necessità che il principio venga adottato dall'industria canadese[61].

Ricercando le tracce del principio nelle decisioni e pubblicazioni dell'OPC si può rilevare che l'autorità si è servita dell'approccio di pbd per interpretare il principio di minimizzazione del Model Code e la natura delle misure di safeguards, con lo scopo di chiarire quali siano le pratiche conformi alla PIPEDA e di condannarne invece delle altre.

Nel 2010, l'OPC ha compiuto un'indagine su Google Street View, ed è emerso che durante la rilevazione fotografica dei territori canadesi Google ha inavvertitamente raccolto delle informazioni riservate sia da luoghi pubblici sia provenienti da abitazioni di privati, perché dotati di rete wireless non protetta[62]. Google Street View è un servizio fornito da Google Inc. dal 2007 che, attraverso delle fotografie montate in successione e raccolte grazie a delle fotocamere su

[61] Ad esempio si veda il Report on the 2010 Office of the Privacy Commissioner of Canada's, Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing, available at <https://www.priv.gc.ca/media/1961/report_201105_e.pdf>, 20: "*The OPC will work with Industry Canada to consider how best to integrate privacy by design principles and PIAs into private sector practices*". L'OPC è l'autorità federale preposta alla promozione e alla protezione della privacy in Canada. Per le informazioni si veda il sito di riferimento: <https://www.priv.gc.ca/en/>.

[62] Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2011-001, available at: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-001/>: "*The central issue concerning the investigation was the unlawful collection of personal information. In May 2010, Google discovered that it had collected payload data from unsecured wireless networks in several countries, including Canada, during data gathering operations for its location-based services. "Payload" data constitutes the core information carried within a transmission unit (or "packet") over the internet. It can, depending on the nature of the communication, contain personal information. As such, our Office focused its investigation on the extent to which payload data collected by Google included the personal information of Canadians*".

automobili, mostra agli utenti del web le strade di moltissime città del mondo con una vista panoramica a 360 gradi[63].

L'OPC ha emesso un lungo reclamo contro Google lamentando le seguenti violazioni della PIPEDA: la raccolta dei dati non è stata limitata a quanto fosse necessario agli scopi identificati dall'organizzazione; è stata operata senza una previa definizione e denuncia degli scopi; è avvenuta senza che gli individui ne fossero a conoscenza o che potessero esprimere il loro consenso[64].

Tra le righe del compliant dell'OPC si afferma che gli incidenti per la privacy dei canadesi potevano essere evitati dalla preventiva predisposizione di adeguate procedure, garanzie e da corrette privacy policies[65]. Sul punto, come si legge nel case summary dell'OPC, Google ha deciso di rivedere le misure a protezione della privacy intervenendo a livello di progettazione dei prodotti e dei servizi e di formazione dei propri dipendenti[66]. La società ha così implementato diverse misure applicative del principio di privacy by design[67].

È interessante sottolineare che nel progetto di intervento è stata prevista la stesura di "Privacy Design Documents" da parte dei dipendenti della società, per assicurare che al suo interno gli ingegneri e gli sviluppatori fossero in grado di stimare l'impatto sulla privacy dei prodotti e dei servizi realizzati, dall'inizio della progettazione fino al loro lancio sul mercato, dovendoli poi aggiornare

---

[63] Per le norme sulla privacy di Google Street View si veda in Rete: <https://www.google.it/intl/it/streetview/privacy/>.

[64] PIPEDA Case Summary #2011-001, cit.: "*On all three allegations - limiting collection, identifying purpose, and consent - our Office found Google to be in contravention of the Personal Information Protection and Electronic Documents Act, and concluded that the Commissioner-initiated complaints were well-founded*".

[65] CAVOUKIAN, JONES HARBOUR, *White paper for regulators, decision-makers, policy-makers*., cit., 186.

[66] PIPEDA Case Summary #2011-001, cit., par. 55: "*Google submits that it continues to design privacy protections into all of its products and services. It has also stated that its employees will continue to receive orientation and code-of-conduct training that includes a privacy and data-security component. In order to avoid a recurrence of this incident, Google has further committed to reviewing its product launch procedures, code review procedures and other such internal processes to ensure appropriate oversight for privacy concerns*".

[67] CAVOUKIAN, JONES HARBOUR, *White paper for regulators, decision-makers, policy-makers*., cit., 186-187: "*After the Privacy Commissioner issued her findings and recommendations in October 2010, Google agreed to implement key privacy by design-related recommendations, including: implementing a system for tracking all projects that collect, use or store personal information and holding the engineers and managers responsible for those projects accountable for privacy; requiring engineering project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure that engineering and product teams assess the privacy impact of their products and services, from inception through to launch; assigning an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents, and their review by the appropriate managers; and piloting a review process whereby members of Google's Privacy Engineering, Product Counsel and Privacy Counsel teams review proposals involving location-based data, as well as the software programs that are to be used for the collection of data*".

costantemente[68]. Solo grazie agli interventi citati la società statunitense è riuscita dimostrare di aver provveduto a garantire la conformità delle sue pratiche alla PIPEDA e così a porre fine alla controversia con l'OPC[69].

Nel case summary si ritrova chiaramente il principio di privacy by design. Questo caso dimostra che le autorità garanti per la privacy possono stimolare le imprese nell'adottare le migliori soluzioni e implementare le loro garanzie fin dall'origine dei prodotti e dei servizi, anche quando non è presente nell'ordinamento giuridico una norma esplicita e diretta in questo senso; certo è che il lavoro interpretativo richiede l'utilizzo di vari espedienti indiretti e non scontati e che l'elaborazione di soluzioni sempre innovative è lasciata in gran parte alla discrezionalità delle società commerciali.

Per fornire una guida interpretativa alle società e agli altri soggetti coinvolti per la protezione della privacy, l'OPC elabora ed aggiorna annualmente degli Interpretation Bulletins sui principi della PIPEDA[70]. Queste interpretazioni dell'OPC non sono legalmente vincolanti, ma fungono da guida per comprendere la conformità alla legge[71]. Per quanto riguarda le misure di sicurezza, si può rilevare che la privacy by design è un principio sotteso e implicito quando l'autorità affronta i casi in cui sono presenti le tecnologie di Internet[72]. Ad esempio, l'OPC afferma nel Bollettino sulle safeguards che le organizzazioni che conservano le informazioni online devono assicurare che i

---

[68] *Ibidem,* par. 65: "*In November of 2010, Google began requiring engineering project leaders ("Tech Leads") to draft, maintain, submit and update Privacy Design Documents for each and every project they are responsible for. If the project operates as intended, it will ensure mandatory privacy documentation for user-facing products, experimental projects, and services that are internal to Google. These documents should play an important role in ensuring that engineering and product teams assess the privacy impact of their products and services from inception through launch. Specifically, the Privacy Design Documents will require Google's Tech Leads to describe the types of data that their projects collect, handle or process as well as how that data is to be protected. Privacy Design Documents are to be regularly reviewed by managers and will be considered during employee performance review cycles. Google expects the first set of manager reviews to occur in 2011*".

[69] *Ibidem*, par. 69: "*All in all, our Office is satisfied that, once fully implemented, Google's proposed remedial measures as set out above will meet the privacy issues underscoring our recommendations*".

[70] Per l'elenco dei Bollettini si veda in Rete: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/>.

[71] Office of the privacy Commissioner of Canada, OPC, Interpretation Bulletin: Safeguards, June 2015 available at: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/>: "*These Interpretation Bulletins are not binding legal interpretations, but rather, they are intended as a guide for compliance with PIPEDA*".

[72] Office of the privacy Commissioner of Canada, OPC, Interpretation Bulletin: Safeguards, 2015 available at: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/>. I casi in cui si è rilevato l'utilizzo implicito dell'approccio sono contenuti nella categoria interpretative "Internet and Technology".

dati siano adeguatamente protetti da terzi non autorizzati attraverso l'utilizzo di password o protezioni di crittografia, che, si intuisce dal caso citato dall'autorità, devono essere adottate in ogni tempo[73]. Ciò vale anche per la conservazione su dispositivi mobili: le organizzazioni devono assicurare che gli strumenti siano correttamente sicuri in ogni momento, criptati, protetti da password e bloccati[74]. Tutte queste misure sono tipicamente delle soluzioni di privacy by design e il fattore temporale di implementazione è aderente con i suoi ideali.

Nello stesso Bollettino l'OPC ha riportato un altro caso in cui sono state richieste maggiori e più affinanti misure tecniche di sicurezza ad una famosa società statunitense. Nel 2012 l'OPC ha intrapreso un'indagine sull'applicazione per messaggi denominata WhatsApp. Secondo l'interpretazione dell'autorità canadese, le organizzazioni che trasferiscono via Internet delle informazioni contenenti dati personali sensibili devono impiegare sufficienti e adeguate tutele, come ad esempio la criptazione[75]. Invece, a parere dell'OPC la società, oggi appartenente al proprietario di Facebook, aveva creato un'applicazione in cui i messaggi potevano essere facilmente intercettati e letti di nascosto[76]. Perciò, applicando il settimo principio sulla sicurezza, le informazioni non risultavano protette con misure adeguate al loro carattere sensibile e non erano volte a prevenire l'accesso non autorizzato, la perdita, il furto e la copia[77]. In parte grazie alle osservazioni dell'OPC, nel 2012 è stato aggiunto a WhatsApp un protocollo di criptazione[78]. Successivamente alla verifica di conformità

[73] *Ibidem*: "*Organizations that store personal information online must ensure that the information is adequately protected from unauthorized individuals through the use of passwords or encryption protection*". Sotto il principio l'OPC cita il PIPEDA Case Summary #2009-017.

[74] *Ibidem*: "*Organizations that use portable electronic devices to store personal information must ensure that the devices are properly secured at all times. Devices with personal information on them must be encrypted, password protected and backed* up". Il caso citato sotto il principio è: PIPEDA Case Summary #2008-393 Laptop theft at bank and long delay before informing victims were both avoidable.

[75] *Ibidem*: "*Organizations that transfer information containing sensitive personal information via the Internet must employ sufficient safeguards such as data encryption*. Il caso WhatsApp è PIPEDA Report of Findings #2013-001 Investigation into the personal information handling practices of WhatsApp Inc.

[76] PIPEDA Report of Findings #2013-001, cit., par. 86: "*Based on a technical analysis of the application, our Office initiated a complaint to investigate whether WhatsApp was adequately protecting personal information, in contravention of Principle 4.7 of Schedule 1 of the Act. More specifically, it was alleged that messages sent and received using the WhatsApp service were not being encrypted, rendering personal information contained in such messages subject to eavesdropping or interception*".

[77] *Ibidem*, par. 90: "*In making our determination on this issue, we applied Principle 4.7 of Schedule 1 of the Act. Principle 4.7 requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 provides that security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification*".

[78] *Ibidem*, par. 93-94: "*In partial response to our concerns, in September 2012 WhatsApp began adding protocol encryption to its mobile messaging service. If properly applied, the end-to-end encryption would appropriately safeguard messages from eavesdropping or interception. As at the time our investigation concluded, WhatsApp had implemented encryption for several*

dell'autorità, il reclamo è così stato ritirato[79]. Se oggi si apre una chat di questa applicazione si può leggere la frase seguente: "i messaggi che invii in questa chat e le chiamate sono ora protetti con la crittografia end-to-end"[80]. Ancora una volta l'adozione della pbd è stata sollecitata da un'interpretazione attenta e pragmatica di un'autorità garante.

Ad oggi molti colossi di Internet sono stati costretti ad adeguarsi alle varie prescrizioni delle autorità di diversi ordinamenti per non subire dei pesanti svantaggi economici, o essere condannati dall'opinione pubblica. Eppure, si può rilevare che le violazioni della riservatezza sono ancora estremamente diffuse e il bilancio induce a pensare che c'è ancora molta strada da fare per proteggere efficacemente i diritti degli individui. Il punto di partenza è sempre il diritto e il suo potere di conformare la tecnologia alle sue regole.

4. Un prototipo di norma disciplinante la privacy by design

Ann Cavoukian, in qualità di Information e Privacy Commissioner dell'Ontario, e Pamela Jones Harbour, Former Federal Trade Commissioner, hanno elaborato nel 2011 un contributo intitolato *White paper for regulators, decision-makers, policy-makers*[81]. In questo paper, frutto dell'interessante collaborazione tra una Commissaria candese e una statunitense, si evidenzia l'importanza del ruolo del diritto per l'applicazione del principio di privacy by design.

Nel dettaglio, si delineano le caratteristiche di un framework ideale che possa comprendere al suo interno il principio di pbd. Innanzitutto, si specifica che l'approccio regolatorio di un legislatore deve comprendere delle forme di autoregolamentazione per i soggetti commerciali, delle leggi settoriali, una legislazione onnicomprensiva sulla privacy e delle misure sulla privacy contenute in più leggi generali su altre tematiche[82].

Le leggi settoriali dovrebbero essere emanate soprattutto negli ambiti in cui sono presenti tipologie di aziende di recente introduzione nel mercato o sono adottate scelte tecniche del tutto nuove, affinché la privacy by design e i

---

devices, including Nokia's S40, Research in Motion's BlackBerry, Apple's iPhone, and all Windows and Android based phones".

[79] *Ibidem*, par. 99: "*Based on the results of our investigation, and as at the time that our investigative work ended, the security safeguards employed by WhatsApp appeared to be commensurate with the sensitivity of personal information at risk. As such, we find the complaint on the matter of transmission security to be well founded and resolved. We nonetheless encourage WhatsApp to remain vigilant when protecting personal information in light of a constantly changing threat environment*".

[80] Per le informazioni si veda il sito sulla sicurezza dell'applicazione: <https://www.whatsapp.com/security/?l=it>.

[81] CAVOUKIAN, JONES HARBOUR, *White paper for regulators, decision-makers, policy-makers*., cit.

[82] *Ibidem*, 175: "*Regulatory approaches, for our purposes here, may include certain forms of self-regulation, sectoral privacy laws, omnibus privacy legislation, and, of course, privacy provisions contained in more general laws*".

suoi standard possano essere applicati dal primo stadio dello sviluppo tecnologico ed organizzativo e così vengano assorbiti molto più facilmente[83].

La legislazione onnicomprensiva, invece, è un ottimo strumento per descrivere lo stato ideale che deve assumere la protezione del dato personale. In merito la privacy by design può ispirare sia il momento in cui il dato inizia ad essere raccolto, sia tutto il suo "ciclo di vita", creando una tutela completa ed efficace[84].

Tutto ciò risulta in sintonia con le considerazioni esposte in relazione alle prospettive future della pbd: la norma giuridica deve essere il più possibile chiara, vincolante ed applicabile al maggior numero di situazioni possibili, generale e anche settoriale, sufficientemente dinamica e soggetta ad aggiornamenti periodici. In un certo senso anche la regola deve essere "progettata" dal legislatore, magari coadiuvato da figure esperte sulla tematica.

Se si tiene conto però degli ordinamenti di provenienza delle due autrici, si intuisce che nei confronti di questi la proposta è molto innovativa e tende a considerare la pbd non solo come un principio da implementare nelle pratiche commerciali e da inserire nella legislazione, ma anche come uno strumento per migliorare l'intero quadro normativo della privacy e renderlo più completo e coerente.

In allegato al White Paper si trova un'appendice denominata "*what pbd could look like as part of a legal framework*", la quale, come il titolo indice a pensare, contiene una norma concreta di privacy by design in cui vengono condensate tutte le riflessioni teoriche esposte[85]. Questa norma, si scrive, è stata elaborata sulla base dei sette principi fondativi di Ann Cavoukian, sul report dell'OPC sul caso Google Street View, sulla Sezione 103 del Commercial Privacy Bill of Rights Act of 2011 e su una legge statale del Massachusetts[86]. Gli elementi appena elencati sono proprio le fonti utilizzate in questo capitolo per tracciare la presenza della privacy by design nei due ordinamenti

---

[83] *Ibidem*, 182: "*One area where sector-specific privacy regulation may be particularly useful is with regard to industries or practices that are in their nascent stages, where standards for the protection of personal information can be set early on, and then be more easily absorbed as part of the initial architecture*".

[84] *Ibidem*, 183: "*Omnibus privacy legislation provides a vehicle for describing a desired end state in terms of how personal information is managed and protected. The principles of Privacy by Design can inform both the end state (e.g. privacy as the default), and the process for arriving at the end state (e.g. end-to-end, full lifecycle protection)*".

[85] *Ibidem,* Appendix B: *What pbd could look like as part of a legal framework*, 191-192.

[86] *Ibidem*, 191: "*This draft legal framework is offered to stimulate discussion on how to provide a flexible but enforceable legal framework for PbD, for example as part of a safe harbor initiative or an omnibus privacy statute. It draws on Commissioner Cavoukian's 7 Foundational Principles: Implementation and Mapping of Fair Information Practices; the Privacy Commissioner of Canada's Google report, PIPEDA Case Summary #2011-001; Section 103 of the Kerry-McCain Commercial Privacy Bill of Rights Act of 2011; and elements of the Massachusetts Data Breach Notification Law and Massachusetts Executive Order 504*".

statunitense e canadese. L'incontro tra le diverse esperienze ha prodotto una lunga norma che risulta la miglior sintesi dell'approccio di privacy by design.

Il primo comma statuisce che:

> *"Each organization shall, in a manner proportional to the organization's size, scope, and resources and the size, type, and nature of the personal information that it collects, implement a comprehensive Privacy by Design program by:*
> *(1) Incorporating necessary development processes and practices designed to safeguard the personal information of individuals throughout the lifecycle of a product, program or service and*
> *(2) Maintaining appropriate management processes and practices throughout the data lifecycle that are designed to ensure that information systems comply with:*
> *(A) Privacy requirements provided for by law;*
> *(B) The privacy policies of the organization; and*
> *(C) The privacy preferences of individuals that are consistent with the applicable mechanisms required or provided to give effect to individual choice*"[87].

Leggendo la prima parte della disposizione è possibile riscontrare la presenza degli elementi tecnici e organizzativi che contraddistinguono la privacy by design: l'incorporazione delle regole deve avvenire sia all'interno dei processi che delle pratiche. In aggiunta, si fa riferimento alla fondamentale fonte legislativa, alle policies all'interno delle aziende e all'importanza delle scelte individuali dell'utente. In poche parole, la pbd risulta condensata in una norma generale e tecnicamente neutrale.

Il secondo comma descrive più in dettaglio quali debbano essere gli elementi di un programma onnicomprensivo sulla privacy by design. Ogni organizzazione dovrebbe stabilire chi siano i soggetti incaricati per l'applicazione del programma di pbd e i processi e le pratiche dovrebbero:

1. Essere applicati alla progettazione dell'architettura e della struttura dei sistemi ICT e delle stesse pratiche commerciali;
2. Descrivere ciascuno degli scopi di base e delle funzioni di questi sistemi, tra le quali vi sono la sicurezza e la protezione dei dati personali, ma non solo;
3. Incorporare la minimizzazione dei dati e provvedere al più alto grado possibile di protezione della privacy, pur perseguendo altri obiettivi e mantenendo tutte le funzioni;

[87] *Ibidem*, 191.

4. Provvedere a questo grado di protezione utilizzando i mezzi migliori per assicurare la sicurezza, la confidenzialità, l'integrità delle informazioni personali, durante tutto il ciclo di vita dei dati, dalla loro raccolta, all'utilizzo, alla conservazione, alla diffusione e alla loro distruzione sicura;
5. Provvedere per quando possibile alla protezione automatica della privacy, in modo che non sia richiesta alcuna azione da parte degli utenti/consumatori per proteggere le loro informazioni personali;
6. Assicurare che la struttura tecnica, i sistemi ICT e le pratiche commerciali, in cui si utilizzano dei dati personali, rimangano ragionevolmente trasparenti e soggetti alla verifica imparziale di tutti i portatori di interessi, tra cui i consumatori, gli utenti e le associazioni;
7. Enfatizzare e mantenere un approccio in cui l'utente è al centro, grazie a impostazioni predefinite a favore della privacy, a notifiche appropriate e altre opzioni user-friendly[88].

L'organizzazione commerciale in supporto a questo programma di pbd deve, ai sensi del terzo comma, provvedere a formare adeguatamente i propri dipendenti sia sulla privacy sia sulla sicurezza, implementare dei sistemi di monitoraggio e tracciamento dei progetti che utilizzano dati personali, elaborare dei Privacy Design Documents per controllare ogni sviluppo dei processi, dei

[88] *Ibidem*, 191-192: "*A comprehensive Privacy by Design program must include the following elements:*
(1) An organization shall establish a Privacy by Design leader and/or team by identifying the appropriate directors, officers, and managers responsible for developing, maintaining, implementing, and updating proactive Privacy by Design processes and practices;
(2) Proactive Privacy by Design processes and practices shall:
(A) Apply to the design and architecture of infrastructure, IT systems, and business practices that interact with or involve the use of any personal information;
(B) Describe each of the core purposes served and main functions delivered by those infrastructures, systems and practices, including but not limited to the provision of security and the protection of privacy in personal information;
(C) Incorporate data minimization and provide the highest degree of privacy protection for personal information possible while serving the other core purposes and delivering the other main functions;
(D) Provide this degree of privacy protection by employing the maximum feasible means needed to ensure the security, confidentiality, and integrity of personal information throughout the lifecycle of the data, from its original collection, through to its use, storage, dissemination, and secure destruction at the end of the lifecycle;
(E) Whenever reasonably possible, provide for that privacy protection automatically, so that no action is required for individual users or customers to protect the privacy of their personal information;
(F) Ensure that infrastructure, IT systems, and business practices that interact with or involve the use of any personal information remain reasonably transparent and subject to independent verification by all relevant stakeholders, including customers, users, and affiliated organizations; and
(G) Emphasize the design and maintenance of user-centric systems and practices, including strong privacy defaults, appropriate notice, and other user-friendly options".

prodotti e dei servizi, e infine assegnare ad un team interno di vigilanza il compito di controllare questi passaggi[89].

Confrontando la norma ideale proposta dalle Commissarie e l'articolo 25 del GDPR, si può affermare che la disposizione europea ha colto nel segno nel prevedere la compresenza di misure tecniche ed organizzative in un modo tecnologicamente neutrale e ha il pregio di riferirsi a criteri puntuali di cui tenere conto al momento del trattamento dei dati. Entrambe le disposizioni sono chiare e sufficientemente generali e lasciano spazio alle particolarità del caso concreto. Sicuramente la versione di pbd contenuta nel paper citato è più completa, ma non si deve dimenticare che l'articolo 25 è inserito in un Regolamento che comprende al suo interno molti altri principi informatori della materia, come la minimizzazione e l'accountability.

Si ritiene, quindi, che la norma del GDPR possa essere considerata un buon punto di partenza per l'introduzione della privacy by design in Europa. Con occhio comparatistico si auspica che l'ordinamento statunitense e quello canadese possano dotarsi al più presto di una norma disciplinante la pbd, per assicurare un'effettiva e maggiore protezione dei dati personali a livello mondiale. I legislatori d'oltreoceano potrebbero assumere come modello la proposta delle due Commissionarie, dato che è il frutto dell'interpretazione delle loro norme positive, per adeguarsi alle esigenze paventate dalla dottrina e dalle loro autorità garanti.

La privacy by design deve passare dalla retorica alla realtà, dall'applicazione in casi singoli ed esemplari alla generalità dei trattamenti dei dati personali.

[89] *Ibidem*, 192: "*In support of a comprehensive Privacy by Design program, an organization must:*
(1) Provide appropriate privacy and security training to its employees;
(2) Implement a system for tracking all projects that regularly collect, use or store personal information;
(3) Require project leaders to draft, maintain, submit and update Privacy Design Documents for all projects in order to help ensure product, program or service teams assess the privacy impact of their products, programs and services from inception through launch; and
(4) Assign an internal audit team to conduct periodic audits to verify the completion of selected Privacy Design Documents and their review by the appropriate managers".

Capitolo 4: Le applicazioni del principio

"Nella società dell'algoritmo svaniscono
garanzie che avrebbero dovuto mettere le persone
al riparo dal potere tecnologico, dall'espropriazione della loro individualità
da parte delle macchine".
Rodotà, Il diritto di avere diritti, 2012.

1. Gli ambiti di applicazione

Il principio di privacy by design impone di considerare la protezione dei dati personali e la riservatezza sin dalla progettazione del prodotto o dell'esecuzione di un servizio. Perciò, l'esigenza di un'applicazione concreta è insita nella sua stessa definizione. Fin dalla prima elaborazione del concetto, Ann Cavoukian ha individuato nove aree chiave di applicazione: la videosorveglianza, l'utilizzo di dati biometrici, i contatori e le reti intelligenti, i dispositivi mobili e quelli per le comunicazioni, le tecnologie di connettività wireless, le tecnologie per la memorizzazione automatica delle informazioni, il monitoraggio remoto dei pazienti con problemi sanitari e la gestione e l'analisi dei big data[1]. Questi settori necessitano particolarmente di maggiori garanzie per i diritti degli individui perché spesso coinvolgono la sfera più intima della persona e così i suoi dati sensibili.

Nel presente capitolo si intende riportare alcune esperienze che hanno già implementato la pbd in alcuni ambiti giuridici, dimostrando che la conformazione della tecnologica al diritto è una possibilità concreta e uno strumento prezioso per una costante innovazione e creatività della scienza. In certi casi si tratterà di esperienze che non hanno considerato esplicitamente la privacy by design, ma che di fatto hanno condotto ad una soluzione espressiva del principio in questione interpretando i principi e le leggi vigenti.

Verrà anche presentato un modello certificatorio da poco attivo in Canada e contraddistinto dal marchio "*privacy certified by design*".

Nell'attesa dell'effettiva applicazione del GDPR sembra necessario studiare le soluzioni di chi ha già impiegato l'approccio per la realizzazione di prodotti e di servizi o ha sviluppato una certificazione; difatti, dal 2018 un titolare del trattamento residente nell'Unione Europea dovrà mettere in atto le misure

[1] CAVOUKIAN, *Privacy by design,* cit., 5: *"9 Pbd Application Areas: CCTV/Surveillance cameras in mass transit systems; Biometrics used in casinos and gaming facilities; Smart Meters and the Smart Grid; Mobile Communications; Near Field Communications; RFIDs and sensor technologies; Redesigning IP Geolocation; Remote Home Health Care; Big Data and Data Analytics".*

tecniche ed organizzative adeguate ai sensi dell'articolo 25 e potrà sfruttare un strumento certificatorio per dimostrare la conformità del suo trattamento ai principi di protezione dei dati fin dalla progettazione e per impostazione predefinita.

1.1 La videosorveglianza

Il problema della sorveglianza generalizzata dei cittadini da parte degli Stati ricorda il progetto di Panopticon del filosofo e giurista settecentesco Jeremy Bentham, che ha elaborato un modello di carcere ideale in cui un unico guardiano può osservare tutti i detenuti senza che questi sappiano se e quali delle loro azioni sono state viste, in modo da condizionarne il comportamento[2]. Due secoli più tardi è il Grande Fratello di Orwell lo specchio di una società totalizzante, in cui l'individuo è completamente privo della libertà e della privacy[3]. Queste opere letterarie mostrano delle situazioni al limite, distanti dalla realtà attuale in cui gli individui hanno perso ogni traccia di libertà e riservatezza.

È noto, grazie alle dichiarazioni dell'informatico Edward Snowden, che in seguito agli attacchi terroristici dell'11 settembre 2001, le agenzie di intelligence degli Stati Uniti hanno posto in essere dei programmi di sorveglianza di massa e hanno raccolto su larga scala i dati di moltissimi utenti dei servizi di comunicazione di tutto il mondo[4]. Il controllo sulle informazioni sembra essere prezioso per prevenire ulteriori attacchi e così proteggere le Nazioni. Non si dimentichi però che per garantire un'efficace verifica del comportamento degli individui è necessario che i sistemi di videosorveglianza siano nascosti e segreti, per evitare che si creino delle asimmetrie e dei falsi positivi o negativi[5]. La segretezza allora non coincide con la libertà degli individui e nel bilanciamento tra la privacy e la sicurezza troppo spesso è quest'ultima che prevale.

Il principio di privacy by design può difficilmente trovare applicazione nell'ambito della sorveglianza di massa perché i dati raccolti spesso non identificano un individuo, ma sono i cosiddetti big data, e il loro trattamento soggiace alle condizioni e ai limiti dell'esigenza di sicurezza degli stati.

---

[2] J. BENTHAM (a cura di M. FOUCALT e M. PERROT), *Panopticum, ovvero la casa d'ispezione*, Marsilio, Venezia, 2002.

[3] G. ORWELL (a cura di L. RUSSO), *1984*, Aesthetica edizioni, Palermo, 1986.

[4] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. Informazione e Informatica*, 2015, fasc.4-5, 698.

[5] B. V. SCHERMER, *Surveillance and privacy in the ubiquitous network society*, 1 *Amsterdam L.F.* 63 (2008-2009), 71: "*In summary we can state that in the future the power of surveillance and its effect on life in the public domain will be greater, while the transparency of surveillance will decrease. This will lead to information asymmetries between the surveyors and those being surveilled. Without proper oversight and checks and balances, surveillance may pose an increased threat to personal autonomy. Up until now, the right to privacy is used to negate any information asymmetries, however, it is unclear whether this will be sufficient in the future*".

È stato affermato, tuttavia, che degli accorgimenti di pbd possono efficacemente essere applicati anche per i sistemi dell'NSA statunitense, perché la videosorveglianza di massa incide eccessivamente sui diritti dei cittadini; così i sistemi federali dovrebbero e potrebbero attenersi ai criteri dell'anonimizzazione, della minimizzazione e dell'immutabilità degli *audit log*[6].

In Canada, grazie alla collaborazione di Ann Cavoukian con due ricercatori universitari, è stato elaborato un sistema tecnologico che assicura l'applicazione dei criteri citati; per l'appunto è stato dimostrato che è possibile progettare la videocamera collocata nelle varie zone della città in modo che i volti dei soggetti registrati non siano identificabili[7]. Questo sistema di criptaggio assicura le esigenze di sicurezza nazionale perché, in caso di necessità, consente una visione completa dell'immagine: la registrazione può essere decriptata da un tecnico e così l'autorità può ottenere le informazioni biometriche per identificare il sospetto criminale, ma solo dopo un'indagine autorizzata della polizia[8].

Un altro esempio offerto dal panorama canadese è il *Privacy-Protective Surveillance*, un sistema di sorveglianza applicativo della pbd, che si compone di tre elementi: un software di intelligenza artificiale che seleziona le attività da riprendere, un sistema di criptazioni nel database che consente di collegare le attività con gli individui colpevoli e poi di svelarle solo quando è richiesto da un giudice, un insieme di modelli di grafici che matematicamente calcolano la probabilità di verificazione degli eventi terroristici[9]. L'utilizzo di questo sistema

---

[6] O. TENE, *New harm matrix for cybersecurity surveillance*,12 *Colo. Tech. L.J.* 391 (2014), 405-406: "*Anonymization, or de-identification, the removal or masking of personal data from a dataset, remains one of the most useful privacy enhancing mechanisms. […] In addition to de-identification, the administrators of monitoring programs should implement data minimization and limit data retention periods. […] An additional technology, which mitigates potential abuses of monitoring programs, is immutable audit logs*".

[7] A. CAVOUKIAN, *Privacy and video surveillance in mass transit systems: a special investigation report – Privacy Investigation Report MC07-6*8, Information and Privacy Commissioner of Ontario, 2008, available at: <http://www.ontla.on.ca/library/repository/mon/21000/279882.pdf>, 12: "*Recent research has shown that it is possible to design surveillance systems in a manner that may successfully address issues of public safety, while at the same time, protecting the privacy of law-abiding citizens. There are a variety of technologies based on digital image processing that are currently being researched and developed for protecting the privacy of individuals appearing in video surveillance footage. As described in the research literature, these approaches are operating as follows: Step 1: object detection and segmentation methods for locating objects of interest, such as human faces, within images and video frames; and Step 2: object obscuration or securing methods, which after the completion of step 1, manipulate the pixel data so that some or all viewers of the surveillance footage are unable to discern the private object content (which one is seeking to protect from viewing)*".

[8] *Ibidem*, 13.

[9] A. CAVOUKIAN A., K. EL EMAM, et al., *Introducing Privacy-Protective Surveillance: achieving privacy and effective counter-terrorism*, Information and Privacy Commissioner, Ontario, 2013, available at: <www.privacybydesign.ca>, 7-8: "*As illustrated in Figure 1, PPS consists of three main technological components: 1) intelligent virtual agents designed to search for suspicious activities online or in transactional databases, and once detected, fag that activity, while encrypting any personal information associated with those activities; 2) a system utilizing*

assicura la protezione dei dati personali raccolti lasciando intatte le esigenze di sicurezza, poiché le telecamere catturano le immagini degli individui, ma l'utilizzo dell'intelligenza artificiale scherma le situazioni che non sono sospette e non devono essere controllate.

Se è vero che può essere difficile intervenire a livello tecnico per la sorveglianza di massa, quantomeno è possibile farlo a livello organizzativo; infatti, possono essere elaborate delle policies che tengano sì conto delle esigenze di sicurezza, ma che informino chiaramente il cittadino di ogni caratteristica precisa del trattamento dei dati, tra cui le finalità, e limitino l'accesso agli stessi a pochi soggetti incaricati[10].

Esistono, comunque, dei sistemi di videosorveglianza di minor impatto, ma ugualmente lesivi dei diritti dei soggetti controllati, a cui si possono più facilmente applicare le soluzioni di pbd. È il caso delle videocamere installate sui luoghi di lavoro o negli istituti pubblici, che registrano le immagini dei lavoratori dipendenti e degli utenti o consumatori dei servizi. Proprio in questo contesto si possono segnalare due diverse applicazioni della privacy by design.

Un gruppo di informatici, al cui contributo si rimanda, ha elaborato una soluzione per evitare che le videocamere riprendano i dipendenti nei luoghi di lavoro: un insieme di autenticazioni e chiavi crittografiche che sfruttano i dispositivi mobili di questi soggetti possono impedire al sistema di sorveglianza di registrare i loro movimenti[11]. Si può pensare a dei sensori che entrano in connessione con la videocamera e inviato il segnale di non riprendere il soggetto che indossa il dispositivo. In questo modo possono essere evitate le problematiche della conformità delle installazioni con i diritti dei lavoratori, come accade in Italia per le garanzie previste dallo Statuto dei Lavoratori[12]. Per

---

Secure Multi-Party Computation methods, such as "homomorphic encryption, to allow for the interrogation and analysis of the encrypted data, to determine the potential links between various activities and individual(s); and 3) probabilistic graphical models, such as Bayesian networks, to perform inferential analysis on the anonymous data in order to calculate the probability of a terrorist threat, given the evidence revealed from the linked suspicious activities. Is probability will then be used for the purpose of soliciting a warrant to decrypt the personally identifiable files in order to allow for further investigations to be carried out".

[10] Si vedano le linee guida in A. CAVOUKIAN, *Guidelines for the use of video surveillance cameras in public places,* Information & Privacy Commissioner, Ontario, Canada, 2007, available at: <http://www.ontla.on.ca/library/repository/mon/20000/277889.pdf>.

[11] P. BIRNSTILL, S. BRETTHAUER, S. GREINER, E. KREMPEL, *Privacy-preserving surveillance: an interdisciplinary approach*, 5 *IDPL* (2015), 300: "*In order to enforce (group) identity-based privacy requirements, eg, hiding employees in the video surveillance process, we need to enable respective persons to authenticate themselves with the system. We propose to use a two-step authentication scheme using a mobile communication device, eg, a smart phone or tablet. First, a cryptographic authentication is performed over a wireless network, authenticating the mobile device as belonging to somebody from the group of employees (or, as the case may be, a particular person). In the second step, the surveillance system replies with a short-lived graphical code, which is easy to recognize for surveillance cameras*".

[12] Legge 20-05-1970, n. 300 Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento in G.U. n. 131

l'appunto il Garante Privacy in una verifica preliminare su un sistema installato da una società trentina ha espresso l'esigenza che la privacy by design venga adottata nell'ambito della videosorveglianza e della geolocalizzazione dei lavoratori perché è espressione del principio di necessità del Codice Privacy[13]. Il principio è stato così utilizzato dall'autorità per verificare le caratteristiche del trattamento dati personali dei dipendenti, effettuato per la finalità di rilevazione delle presenze nell'orario lavorativo: la pbd può essere efficacemente impiegata in questo contesto per tutelare maggiormente la privacy dei lavoratori.

Un'altra applicazione di privacy by design in tema deriva direttamente da una fonte normativa. La Provincia Autonoma di Bolzano ha di recente approvato il Regolamento per l'utilizzo del sistema integrato di videosorveglianza degli uffici centrali[14]. L'articolo 6 del Regolamento prevede che il ciclo di vita dei dati personali raccolti dal sistema integrato di videosorveglianza della Provincia sia rispettoso del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita, in relazione alla legalità, necessità, finalità, proporzionalità, completezza, pertinenza e non eccedenza del trattamento[15]. I sistemi, dunque, dovranno essere conformati alla

---

del 27-05-1970, in Rete: <http://normattiva.it/>. L'articolo 4 dello Statuto vieta l'uso di impianti audiovisivi e apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.

[13] Si veda Garante per la Protezione dei Dati Personali, Verifica preliminare - Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze dell'8 settembre 2016, doc. web n. 5497522, in Rete: < http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5497522>:
"*Con riguardo alla necessità, pertinenza e non eccedenza dei trattamenti che saranno effettuati attraverso il prospettato sistema, risulta in ogni caso necessario tener conto dei possibili errori nella rilevazione del dato relativo alla posizione geografica - dovuti sia ai limiti di accuratezza dei sistemi di geolocalizzazione (come verificato anche nel corso dell'istruttoria) sia alla diversa qualità dei ricevitori GPS installati sui dispositivi mobili - apportando, nella prospettiva della "privacy by design", alcuni correttivi in attuazione del principio di necessità (cfr. art. 3 del Codice). Si osserva inoltre che, rispetto ai sistemi ordinari di rilevazione delle presenze - tramite i quali l'informazione sulla posizione geografica del lavoratore, ricavata indirettamente dalla posizione del lettore dei badge o dalla collocazione del foglio firme, è statica e invariabile -, l'informazione geografica rilevata attraverso la descritta applicazione è differenziata e specifica, sia per l'incidenza dei menzionati margini di errore dei sistemi sia perché ciascun lavoratore, rispetto allo stesso evento (entrata e uscita), effettuerà inevitabilmente la timbratura virtuale all'interno di una coordinata geografica ogni volta diversa (seppur relativa alla medesima area comprendente la sede di lavoro). Si ritiene, pertanto, che in relazione alle finalità perseguite dalle società il sistema debba cancellare le coordinate geografiche della posizione del lavoratore, avendo verificato preventivamente, al fine di scongiurare possibili abusi, l'associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore e conservando, eventualmente, il solo dato relativo alla predetta sede di lavoro*".

[14] Bolzano - Provincia autonoma Delib. G. P. 26/07/2016, n. 846, Approvazione del Regolamento per l'utilizzo del sistema integrato di videosorveglianza degli uffici centrali della Provincia autonoma di Bolzano, pubblicata nel B.U. Trentino-Alto Adige 2 agosto 2016, n. 31.

[15] *Ibidem*, art. 6 Trattamento dei dati: "*L'intero ciclo di vita dei dati personali trattati dal sistema integrato di videosorveglianza della Provincia, a partire dalla raccolta, nonché durante il trattamento e fino alla cancellazione, deve rispettare il principio della "protezione dei dati fin dalla progettazione" e "della protezione per impostazione predefinita" (rispettivamente " privacy by design" e " by default"), con particolare riferimento ai principi di legalità, necessità, finalità, proporzionalità, completezza, pertinenza e non eccedenza. 2. Il trattamento dei dati personali*

privacy by design, per proteggere efficacemente i diritti dei dipendenti pubblici e questa applicazione è in fase di elaborazione. La natura delle soluzioni che verranno adottate potrebbe fornire un modello virtuoso applicabile anche in altre amministrazioni italiane: la privacy by design non vuole essere un approccio esclusivo del settore privato, ma deve e può essere implementata anche dalle imprese e dalle autorità del settore pubblico.

1.2 L'ambito sanitario

Un contesto in cui la privacy by design è stata impiegata in modo più diffuso è il settore medico-sanitario. Le tecnologie dell'informazione applicate al campo della salute, le *Health Information Technologies*, consentono di predisporre una cura individualizzata sulla base delle caratteristiche del paziente e di progredire più velocemente in ambito di ricerca biomedica e farmaceutica[16]. I dati raccolti sono sensibili perché sono idonei a rivelare lo stato di salute del soggetto interessato; perciò l'attenzione sulla sicurezza deve essere molto elevata.

Un'implementazione della privacy by design in ambito medico è fornita dalla Germania, in cui è stata sviluppata una smart card elettronica per identificare il cittadino quando usufruisce dei servizi del sistema sanitario; la carta contiene i dati amministrativi del paziente ed è stata progettata anche per raccogliere le informazioni sulla salute e sugli esami effettuati o le prescrizioni necessarie[17]. È evidente che questo strumento debba poter essere utilizzato facilmente ed in modo sicuro e che la sua progettazione debba aver tenuto conto delle possibilità di discriminazione tra i soggetti dovute all'utilizzo di dati sensibili[18]. È stato rilevato, però, che l'obiettivo dell'utilizzo della privacy by design in questo contesto non possa essere solo la sicurezza dei dati, ma debba riguardare anche l'impossibilità di creazione di profili sui pazienti e di utilizzo dei dati biometrici per l'identificazione degli stessi da parte delle autorità

---

del sistema è consentito solo nei limiti previsti dal presente regolamento alle persone fisiche incaricate per iscritto ai sensi dell'art. 2, comma 1, lettera f). 3. Ogni incaricato deve: - operare sotto la diretta autorità del titolare del trattamento o del responsabile (anche esterno), attenendosi alle istruzioni impartite; - effettuare le operazioni del trattamento esclusivamente nell'ambito consentito; - rispettare il segreto d'ufficio".

[16] PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., 305-306.

[17] P. SCHAAR, *Privacy by design*, 3 *IDIS*, 267 (2010), 268: "*For several years now, Germany has been preparing to introduce an electronic health card (elektronische Gesundheitskarte, eGK) a smart card with an embedded microprocessor which allows additional functions, in particular verifying one's digital identity within the telematics infrastructure of the health-care sector. The smart card will initially contain the cardholder's administrative data which are already on the magnetic health insurance card. The possibility to store additional data (such as prescription drug records, emergency medical information, electronic patient records) is to be added later*".

[18] *Ibidem*, 269: "*All users-patients, insured persons and members of the health professions must be able to use the systems securely and easily*". 270: "*Particularly when designing systems, it is important to make sure that the new technology does not discriminate against elderly or ill persons*".

e delle società commerciali, per evitare che si realizzino diversi e ulteriori interessi grazie allo sfruttamento dei comportamenti e dei movimenti degli individui[19].

La smart card tedesca in realtà è stata progettata non solo per consentire ai cittadini tedeschi di usufruire dei servizi connessi alla salute, ma è anche un sistema che consente un'identificazione sicura con riguardo ad altri servizi pubblici, come il collocamento per la ricerca di un posto di lavoro[20]. Il sistema denominato ELENA (*electronic proof of earnings),* è stato progettato secondo il principio di privacy by design: l'utente per accedervi deve innanzitutto ottenere una firma elettronica da un organismo certificatore, in modo che la sua identità sia verificata, così come ad esempio la sua maggiore età, e poi la carta viene assegnata dall'autorità competente; il database centrale non contiene i dati identificativi dell'individuo perché il processo di registrazione collega l'identità digitale con la persona reale solo sulla base del numero fornito dall'organismo esterno, così la privacy del soggetto è protetta al massimo grado e l'autorità non può monitorarlo[21]. Questo modello è stato criticato perché è sì sicuro, ma richiede la raccolta di un'enorme quantità di dati del cittadino; si è scritto, infatti, che la privacy by design non dovrebbe condurre solo all'elaborazione di soluzioni sempre più innovative e protettive dei dati personali, ma anche alla minimizzazione della raccolta fin quanto è possibile[22].

---

[19] *Ibidem*, 271: "*But PbD does more than ensure data security; Privacy by Design also means collecting and processing as little personal data as possible (principle of data minimization). With regard to the new ID card, this could mean making it impossible to save event and localization data, so that no data-related profile can be created "on" the ID card. Neither past checks of biometric data conducted by government officials nor business contacts using the identity verification function may be retrieved from the relevant zone of the chip and certainly not retrieved and stored by the other zone. This prevents data from being generated when the new ID card is used in different ways and from being used to compile profiles of movement or behaviour*".

[20] KREBS, *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* cit., 6: "*A second example of a system to which PbD principles have been applied is the 'ELENA' system in Germany. It stands for 'elektronischer Entgeltnachweis' (electronic proof of earnings) and refers to a database system in Germany designed to store income information for all individuals employed in Germany for the purpose of streamlining applications for certain social benefits*".

[21] *Ibidem,* 6: "*ELENA as a process and systems was designed as follows: Prior to applying for a certain benefit, an applicant would first obtain an electronic signature card with a smart chip containing a from a qualified electronic signature from a certification service provider. This step provides proof of an individual's identity. This unique signature card is then registered with the appropriate authority. The 'registry process' then links the certificate ID with the social security number of the applicant. On the ELENA database, then, employee personal data is not linked to the social security number of the applicant, but to the ID number of the certificate for the registered chip card. The card itself contains no information other than the name of the applicant and ID number of the registered chip card. All other information is stored in the central ELENA database*".

[22] SCHAAR, *Privacy by design*, cit., 273: "*The example of ELENA also demonstrates that PbD should not be limited to developing clever technical solutions and incorporating them into systems. It is equally important to examine very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary. The tendency to*

Un'altra tecnologia esistente in ambito sanitario è il *Radio Frequency Identification* (d'ora in avanti: RFID), strumento sviluppato per consentire l'identificazione del paziente, delle apparecchiature e dei farmaci che utilizza, e per monitorare il flusso dei dati collegati[23]. L'RFID sfrutta i segnali radio inviati dal device e consente un monitoraggio a distanza del paziente. Per poter funzionare correttamente, il sistema deve poter inviare e collegare le informazioni sulla salute del soggetto, che sono dati identificabili e sensibili.

In Canada è stata implementata una soluzione di RFID compatibile con il principio di privacy by design grazie ad un progetto realizzato dalla nota società informatica HP e ad un'architettura del codice particolarmente attenta[24]. Dal punto di vista organizzativo, sono state formalizzate delle procedure specifiche per le varie fasi di raccolta dei dati della tecnologia RFID: ciascuno stadio dovrebbe essere sottoposto alla propria analisi dei rischi sul modello del Privacy Impact Assessment (PIA)[25].

La collaborazione dell'IPC con delle società private ha consentito anche la progettazione di un sistema di monitoraggio remoto che collega un mobile device utilizzato a casa dal paziente con un'interfaccia online gestita dal suo medico di riferimento: l'Intel Health Guide riduce la necessità di recarsi in ospedale, diminuisce le visite a domicilio, consente un intervento immediato in caso di precarie condizioni di salute o di aggravamenti e assicura il paziente di essere adeguatamente curato[26]. Il progetto è stato realizzato considerando la protezione della privacy dal primo stadio di sviluppo del device; infatti il dispositivo contiene alti standard di sicurezza, sistemi di autorizzazioni doppie e

---

reproduce increasingly complicated bureaucratic systems exactly in information technology can be seen in other IT processes and can lead to major problems for data protection. This risks exists even when great efforts are made to ensure data protection and prevent data misuse".

[23] PASCUZZI (a cura di), *Il diritto dell'era digitale*, cit., 315.

[24] INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, HEWLETT-PACKARD (HP), *RFID and Privacy Guidance for Health-Care Providers*, 2008, available at: <http://www.ontla.on.ca/library/repository/mon/20000/279038.pdf>, 6.

[25] *Ibidem*, 14.

[26] INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, INTEL, GE HEALTHCARE, *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design***,** 2009, available at: <http://www.ontla.on.ca/library/repository/mon/23011/296578.pdf>, 14: "*Another home health technology that is currently in the marketplace offers an excellent case study for the Privacy by Design framework. The Intel Health Guide is a remote patient monitoring system that combines an in-home patient device with an online interface that allows clinicians to remotely manage care. From the health care provider perspective, remote home health care technologies can reduce hospitalization and readmission rates by allowing clinical staff to identify changes in patients' health before conditions become acute, to increase patient compliance with disease management programs, and to offer cost-effective extended care to more patients by allowing clinicians to assist patients without in-person visits. They also provide health care organizations with an additional tool to cope with the challenges of chronic care and to increase efficiency. From the patient perspective, remote health care tools allow patients to become more engaged and proactive in their cases and provide health care providers with more informed and personalized information. The Intel Health Guide offers several features that provide many of the benefits available from remote home health care technologies*".

di criptaggio molto elaborati e limiti stringenti per l'accesso ai dati sensibili[27]. Soltanto il paziente e il suo medico possono vedere i dati raccolti e anche se i dispositivi utilizzano la rete Internet per trasmettere le informazioni, queste non vengono registrate nei server della Intel. Tutto ciò dimostra ancora una volta l'importanza dell'approccio interdisciplinare e del lavoro delle Autorità Garanti con le società private per la creazione di soluzioni efficaci. Un principio del diritto per poter essere applicato richiede una buona collaborazione tra tutti i soggetti coinvolti: il legislatore, le autorità e il settore privato.

Un'esperienza che non ha considerato esplicitamente la privacy by design, ma che di fatto ha condotto ad una sua applicazione deriva da una sperimentazione in Italia del Fascicolo Sanitario Elettronico (d'ora in avanti: FSE). L'FSE è in generale un'infrastruttura informatica per la gestione dei dati da parte delle aziende sanitarie, sviluppata per potenziare i loro servizi[28]. Questo strumento è stato implementato sia a livello internazionale che nazionale in varie e diverse modalità[29]. Nel territorio italiano esistono alcune sperimentazioni già avviate, tra cui il sistema "TreC – Cartella Clinica del Cittadino" sviluppato dalla Provincia Autonoma di Trento[30]. Il progetto ha prodotto una piattaforma di servizi *e-care* molto innovativa, perché dedica un ruolo importante al paziente, che è parte integrante del sistema di gestione delle informazioni idonee a rivelare il suo stato di salute[31]. Questo sistema è stato progettato sin dall'inizio per garantire alti livelli di sicurezza dei dati sensibili coinvolti e per evitarne un utilizzo improprio; i meccanismi protettivi sono stati implementati già dalla creazione dell'architettura informatica, tramite l'uso di soluzioni hardware e software, costantemente aggiornate e monitorate, e la previsione di un sistema di registrazione e autentificazione doppia molto accurato[32]. In aggiunta, l'informativa sulle caratteristiche del trattamento di dati personali, l'interfaccia, nonché la spiegazione delle caratteristiche dei servizi erogati tramite questo trattamento, è molto chiara, diretta e scritta con un linguaggio comprensibile al comune cittadino[33]. La previsione di misure tecniche fin dalla progettazione del servizio e l'utilizzo di un approccio il più possibile user-friendly sono sintomo dell'adozione del principio di privacy by design, seppur non sia stata una scelta dovuta ad una prescrizione normativa. Ciò dimostra che l'approccio di privacy by design è stata considerata una

[27] *Ibidem*, 15.
[28] P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, Quaderni dei Dipartimento di Scienze Giuridiche, Trento, 2011, 1.
[29] *Ibidem*, 57-82.
[30] *Ibidem*, 61.
[31] *Ibidem*, 62.
[32] Per le informazioni si veda in Rete la spiegazione dei meccanismi di sicurezza del sistema TreC sul sito di riferimento del progetto: <https://trec.trentinosalute.net/sicurezza;jsessionid=7865A11B92A391973EFABE55B2A5DCEB>.
[33] Si veda in Rete: <https://trec.trentinosalute.net/informativa>.

soluzione logicamente necessaria e utile a proteggere le informazioni raccolte, anche prima di una sua consacrazione normativa. Tra l'altro, gli aspetti legati alla sicurezza dell'infrastruttura informatica dell'FSE così come previsti dalle Linee Guida in tema di Fascicolo Sanitario elettronico e di dossier sanitario del Garante Privacy, richiedevano già l'incorporazione nella piattaforma di idonei sistemi di autenticazione, autorizzazione, procedure di verifica, cifratura, tracciabilità degli accessi e di *audit log*[34]. Si tratta sempre di applicazioni della pbd doverose e fondamentali nel campo del trattamento dei dati sulla salute dei cittadini.

Nel futuro l'ambito sanitario sarà sempre più legato all'utilizzo delle *Health Information Technologies*. Progettare queste tecnologie in modo privacy-friendly è doveroso non solo per proteggere la riservatezza e i dati dei cittadini, ma anche per garantire che il diritto fondamentale alla salute sia correttamente esercitabile senza compromettere altri diritti della persona umana.

1.4 I social media

Con il termine "social media" si intendono tutte quelle tecnologie che consentono la condivisone online di contenuti digitali. Ad oggi il social più utilizzato al mondo risulta Facebook, che conta 1.79 miliardi di utenti attivi al mese, con un tendenziale aumento annuale del 17%; invece WhatsApp, l'applicazione che consente l'interscambio di messaggi e chiamate a livello

[34] GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, cit., 142.
Al par. 10 delle Linee Guida in tema di Fascicolo Sanitario elettronico e di dossier sanitario del 16 luglio 2009 in G.U. n. 178 03-08-2009 del Garante per la Protezione dei Data Personali si legge: "*La particolare delicatezza dei dati personali trattati mediante il Fse/dossier impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza (art. 31 del Codice), ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.). Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati devono essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati). Devono essere, inoltre, assicurati:*
• idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
• procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
• individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
• tracciabilità degli accessi e delle operazioni effettuate;
• sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie.
Nel caso di Fse, devono essere, poi, garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti".

globale, grazie all'utilizzo della Rete Internet, è utilizzato da un miliardo di persone ogni mese [35].

I numeri lasciano intuire che il fenomeno dei social non può più essere collegato soltanto alle nuove generazioni, ma riguarda un nuovo modo di comunicare dell'era digitale: le persone sono costantemente interconnesse e tendono a condividere la propria vita online e ad inviare ogni genere di contenuti, di immagini, video, audio, ai loro contatti.

Come si è già illustrato, l'applicazione WhatsApp ha già provveduto a conformarsi alla privacy by design in seguito alle indagini dell'OPC ed ha inserito una funzione automatica che consente di crittografare la chat e impedire ad ogni altro soggetto che non sia il mittente o il destinatario di leggere ciò che viene inviato, possibilità negata anche allo stesso gestore della applicazione. La crittografia end-to-end protegge i messaggi con delle chiavi uniche, disponibili solo nei due dispositivi connessi, ed è possibili verificare l'operatività del sistema con una semplice procedura di sicurezza. Se si entra nella schermata di info contatto si ritrova un codice QR e un numero sottostante di 60 cifre, che devono corrispondere in entrambi i dispositivi del mittente e del destinatario: se i due soggetti sono fisicamente accanto, uno dei due può scannerizzare il codice e il sistema verificherà che la corrispondenza delle chiavi è effettiva, mostrando una spunta verde; se invece essi sono distanti, possono inviare il numero di 60 cifre con un tasto "condividi" che appare sulla schermata, e il suo contatto verificherà la corrispondenza con il codice che vede sul suo dispositivo. Qualora i codici non corrispondessero, il sistema consiglia di aggiornare l'applicazione perché la crittografia è una soluzione automatica per le ultime versioni. La procedura è garantita per tutti e tre i sistemi operativi dei dispositivi mobile: Android, iPhone e Windows Phone[36].

Molti contributi dottrinari hanno cercato di fornire gli strumenti per consentire l'applicazione della privacy by design ai gestori dei social media[37]. In

[35] Si vedano i dati presentati da Facebook e aggiornati al 30 settembre 2016: <https://investor.fb.com/home/default.aspx>.

[36] Le informazioni sono disponibili sul sito dell'applicazione in Rete: <https://www.whatsapp.com/faq/it/general/28030015>.

[37] Tra tutti si veda per i social network, D. N. JUTLA, *Layering privacy on operating systems, social networks, and other platforms by design,* 3 *IDIS* 319 (2010), 339: "*This paper introduces a privacy life cycle concept from the user perspective thereby contributing to the classification theory for online privacy management and technologies. The privacy life cycle of Aware, Act, Detect, and Resolve asserts at least the following: (1) Users' knowledge of privacy issues and readiness to act on protecting privacy change over time and hence pass through different phases, each posing different challenges and opportunities in the changing online environment, (2) Protecting privacy requires different, yet sometimes overlapping, strategies and tools in each life cycle stage, and (3) Protecting a user's privacy continues indefinitely, so the phases will cycle or repeat continuously throughout her/his lifetime, and for those affected (e.g. family members), beyond the lifetime. The second major contribution of the paper is a design for providing privacy protection via layering privacy platforms. The multi-layer privacy technology platforms and their services may map to one or more of the lifecycle phases. Formal privacy platforms from the user perspective currently exist only for the Aware and Act phases. Online*

questo contesto la privacy può incontrare il limite dell'asimmetria informativa: l'utente è poco consapevole di ciò che accade nella Rete quando condivide i suoi contenuti digitali. Si è già accennato che un sistema dovrebbe appunto fornire gli strumenti atti a rendere l'individuo più consapevole e attivo, in modo che possa costruirsi da sé la tutela adatta alla sua aspirazione di riservatezza.

A tal proposito è interessante notare che Google, il cui motore di ricerca processa più di 40.000 searches al secondo, ritiene di aver investito in questi ultimi anni nella creazione di soluzioni il più possibile vicine all'approccio di privacy by design, probabilmente sulla scia delle indagini e dei procedimenti promossi dalla FTC, di cui si è dato conto nel precedente capitolo[38]. L'utente può accedere ad un unico portale per controllare, proteggere e mettere al sicuro il proprio account Google[39]. All'interno delle norme sulla privacy del servizio si nota immediatamente che l'informativa è user-friendly, perché sono inserite molte icone interattive, immagini illustrative e le frasi sono semplici e chiare, anche se a volte fin troppo generali e imprecise[40]. Nella versione estesa delle norme, scaricabile dal sito appena citato, si legge che i servizi Google sono crittografati con un sistema di criptazione SSL per impedire a terze parti di rilevare la pagina di ricerca dell'utente, e i suoi dati di accesso sono garantiti da una funzione di navigazione sicura e sono dotati di limiti stringenti[41]. Tra i principi affermati da Google in materia di privacy è indicato che i suoi prodotti sono sviluppati per soddisfare elevati standard di riservatezza e di protezione dei dati, in modo tale da consentire una gestione delle informazioni semplice ed accessibile a tutti e garantire il rispetto delle leggi e applicare le norme giuridiche[42].

---

technologies are becoming available to add to platforms for the first three phases while the Resolve phase's technology assistance is mainly through information-providing web sites at this time".

[38] Per la mole delle ricerche su Google si veda in Rete: <http://www.internetlivestats.com/google-search-statistics/>.

[39] Per il portale si veda in Rete: <https://myaccount.google.com/?hl=it>.

[40] Per le norme sulla privacy dei servizi Google si veda in Rete la versione italiana: <https://www.google.it/intl/it/policies/privacy/>.

[41] *Ibidem*, nella versione scaricabile dal sito, 5: "*Ci adoperiamo per proteggere Google e i suoi utenti da accessi non autorizzati alle informazioni in nostro possesso e dall'alterazione, dalla divulgazione e dalla distruzione non autorizzate di tali informazioni. In particolare: Crittografiamo diversi nostri servizi utilizzando SSL. Offriamo agli utenti una verifica attraverso due passaggi al momento dell'accesso al loro account Google, nonché una funzione Navigazione sicura in Google Chrome. Esaminiamo le nostre prassi di raccolta, archiviazione e trattamento delle informazioni, comprese le misure sulla sicurezza fisica, per impedire l'accesso non autorizzato ai sistemi. Consentiamo l'accesso alle informazioni personali soltanto a dipendenti, fornitori e agenti Google che devono essere a conoscenza di tali informazioni per poterle elaborare per nostro conto. Tali soggetti devono rispettare rigide obbligazioni contrattuali in merito alla riservatezza e potrebbero essere soggetti a sanzioni o risoluzione del contratto qualora non rispettassero tali obbligazioni*".

[42] Per i principi privacy di Google, si veda in Rete: <https://www.google.it/intl/it/policies/technologies/>, par. 2: "*La nostra ambizione è essere all'avanguardia per quanto riguarda la tecnologia, quindi anche nello sviluppo di strumenti che*

Eppure, le politiche di commercializzazione dei dati adottate dal Google e la poca trasparenza nel trattamento inducono a pensare che le soluzioni presentate siano solo dei piccoli germogli inconsistenti, che devono essere alimentati per crescere e portare frutto. Non c'è alcun dubbio che i rischi per la privacy dei sui utenti siano ancora molto elevati e che c'è la necessità di elaborare delle soluzioni molto più precise e garantiste, sulla scorta delle indicazioni più volte fornite dalla FTC alla stessa società a partire dal caso Google Buzz.

A questo punto si intende analizzare un altro social media diffuso in tutto il mondo: Facebook. Questo servizio di rete sociale è attivo dal 2004 e consiste in una piattaforma online in cui è possibile creare un profilo virtuale per condividere vari contenuti ed esperienze di vita con la propria cerchia di amici. L'essenza di Facebook è l'interscambio di informazioni tra gli individui, ma oggigiorno risulta anche uno strumento rilevante per la diffusione capillare degli annunci pubblicitari, delle notizie giornalistiche e per la comunicazione dei personaggi pubblici. Quando si crea un profilo sulla piattaforma si sottoscrive un contratto identificato dalla dottrina come una licenza di un bene immateriale, ossia una forma contrattuale atipica[43]. Una soluzione che garantirebbe al meglio l'applicazione della privacy by design consisterebbe nell'inserimento del principio nel contratto concluso con l'utente. Ciò verrebbe raggiunto solo se la stessa società decidesse di farlo, perché ovviamente in questo caso vi sono le prescrizioni della libertà contrattuale.

In ogni caso, commentando la Proposta della Commissione Europea, la società ha dichiarato che il principio fa già parte del suo programma di privacy e che la centralità dell'utente è un aspetto fondamentale del suo servizio; tuttavia, essa ha anche affermato che l'applicazione congiunta tra la pbd e la privacy by default è difficilmente realizzabile per una piattaforma di social network[44].

Un interessante contributo suggerisce alla società di adottare delle soluzioni di privacy by design più visibili, come l'inserimento di etichette colorate sulla bacheca notizie che segnalino più chiaramente all'utente quali siano le pagine pubblicitarie suggerite in base alle sue preferenze[45]. Anche in questo

---

consentano agli utenti di gestire le proprie informazioni personali in modo semplice e accessibile, senza sminuire il valore del servizio a loro offerto. Rispettiamo le leggi sulla tutela della privacy e lavoriamo in collaborazione con le istituzioni e i partner del settore per mettere a punto e applicare norme efficaci. Abbiamo progettato Google+ con le cerchie in modo da facilitare la condivisione di contenuti diversi con persone diverse. In questo modo è possibile inserire gli amici in una cerchia, la famiglia in un'altra e il capo in una cerchia tutta sua, proprio come nella vita reale".

[43] F. AGNINO, *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (vedi contratto FB)*, in *Giur. merito*, 2012, fasc. 12, 2557.

[44] FACEBOOK IRELAND, "Facebook's Views on EU Data Protection Regulation", March 30 2012, available at: <http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf>, par. 3.

[45] A. E. WALDMAN*, Privacy, Sharing, and Trust: The Facebook Study*, 67 *Case Western Reserve L. Rev.* 1 (2017), 27: "*Facebook has a long way to go before it could be seen as a privacy-by-*

caso l'applicazione della privacy by design da parte della società di social media più famosa al mondo è superficiale e insufficiente. Essa potrebbe prendere a modello le soluzioni elaborate dalla dottrina per la progettazione del social network Diaspora, la cui architettura applica direttamente i sette principi fondativi della pbd[46]. In caso contrario, si afferma, Facebook rischierebbe di subire un ricorso da parte della FTC per *unfair design*, dal momento che manipola i dati dei suoi utenti, sfruttando la loro fiducia nell'applicazione e li utilizza per soddisfare ingenti interessi economici[47].

Insomma, malgrado appaia manifesta una parziale applicazione della pbd, entrambe le società avrebbero potuto implementare molto di più l'approccio; difatti, esse sono state più volte protagoniste di incidenti per la privacy degli individui e di indagini di autorità garanti o di controllo in tutto il mondo. Un prezioso contributo d'oltreoceano ha analizzato i vari privacy incidents di Google e Fabebook e ha concluso che tutti questi episodi potevano essere evitati dall'applicazione più puntuale della privacy by design, dimostrando che essa può effettivamente proteggere i diritti dei consumatori e che l'adozione delle sue soluzioni è attuabile anche dai social media[48]. Secondo gli autori citati,

---

design adopter. But it could start by designing its News Feed to be more transparent about native advertising. The word "sponsored", which is confusing to many users, should be larger and more obvious, not obscured by a light-colored font and other, richer content. The Associated Press mobile application (Figure 3) is a good model. Standard news articles on the interface are in white text on a black background. A picture associated with the article is on the right; the headline is on the left. Sponsored posts not only reserve the positioning of the picture and headline, they are also prefaced by a bright yellow bar that reads "Paid for by …". Furthermore, a "just in time" pop up privacy notification could notify users that a click on sponsored links will release some information to third parties".

[46] ISLAM M. B., IANNELLA R., *Privacy by Design: Does it matter for social networks?*, IFIP Summer School 2011, International Federation for Information Processing, University of Trento, available at: <http://eprints.qut.edu.au/60607/>, 4: "*We have reviewed Diaspora to analyze whether it follows the PbD principles. The privacy-aware Diaspora Social Network has been investigated in terms of how it follows the PbD principles. Diaspora system has selected randomly but for some consequential reason for evaluation. First of all, Diaspora system grabs the attention by the media and technologists. Some technologist claimed that Diaspora might receive attention by the user for privacy issue and the user might change their might to use the well-recognized Social Network. Therefore, Diaspora can be a possible test case for evaluating PbD principles*".

[47] WALDMAN, *Privacy, Sharing, and Trust: The Facebook Study*, cit., 28.

[48] RUBINSTEIN, GOOD, *Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents*, cit., 1406: "*In sum, the preceding counterfactual analyses suggest that all ten privacy incidents might have been avoided by the application of the engineering and usability principles and related design practices discussed in this Article. This is important for two reasons. First, it strongly supports the claim that privacy by design (when so understood) effectively protects consumer privacy. Second, it also suggests that Part II offers a reasonably comprehensive account of privacy engineering and design practices, at least as measured by these ten incidents*". *Ibidem*, 1413: "*These incidents included five from Google—Gmail, Search, Street View, Buzz, and recent changes to its privacy policy; and five from Facebook—News Feed, Beacon, Facebook Apps, Photo Sharing, and recent changes to its privacy policies and settings. Using engineering and usability principles and practices derived from the research literature and described in Section II.B, we determined that each of these incidents might have been avoided if Google and Facebook had followed these principles and practices. Moreover,*

la prima lezione impartita dai fatti accaduti è che i legislatori devono elaborare norme vincolanti e più chiare dal momento che gli strumenti e le misure innovative sono già presenti nel panorama tecnologico e resta soltanto alle società il compito e la scelta di implementarle[49].

2. Un modello di certificazione

Per concludere questo capitolo applicativo sembra opportuno riportare un esempio concreto di certificazione dedicata all'accertamento della privacy by design; si è detto, infatti, che il GDPR prevede esplicitamente la possibilità di utilizzare lo strumento certificatorio sia per la pbd che per la protezione per impostazione predefinita.

All'articolo 42 del Regolamento 2016/679, come si è già accennato, si incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati, di sigilli e di marchi, da adottare su base volontaria, che non riducono la responsabilità dei soggetti, ma che possono dimostrare la conformità con la normativa, essendo rilasciati da organismi accreditati presso le autorità di controllo o dall'organismo nazionale di accreditamento e raccolti in un registro pubblicato con qualsiasi mezzo appropriato[50]. La certificazione potrà essere rilasciata per un periodo massimo di tre anni, ma potrà essere rinnovata più volte, sempreché sussistano i requisiti idonei ad ottenerla e non sia stata

---

we described in specific detail what the two companies might have done differently in each of the ten cases".

[49] *Ibidem*, 1407: "*Having analyzed what went wrong and what Google and Facebook might have done differently in ten privacy incidents, what have we learned? What lessons does this counterfactual analysis hold for regulators that are now placing bets on privacy by design? The first lesson is that companies and regulators should avail themselves of the rich body of research related to privacy engineering and usability design as described in Section II.B. Too often, regulators recommend that companies "build in" privacy or "design and implement" reasonable privacy controls, without explaining what they mean*".

[50] Cfr. art. 42, co. 1, 3, 4, 5, 8, Reg. 2016/679: "*1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese. 4.5.2016 L 119/58 Gazzetta ufficiale dell'Unione europea. […] 3. La certificazione è volontaria e accessibile tramite una procedura trasparente. 4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56. 5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati. 8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato*".

revocata dalle autorità[51]. Gli organismi di certificazione devono essere in possesso di un livello adeguato di competenze riguardo alla protezione dei dati ed operano il loro servizio a stretto contatto con le autorità; essi devono dimostrare di essere indipendenti e di aver adottato una serie di criteri e procedure fondamentali[52].

[51] Cfr. art. 42, co. 7, Reg. 2016/679: "*7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione*".

[52] Cfr. art. 43, Reg. 2016/679: "*1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi: a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56; b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio (1) conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.*
2. Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se: a) hanno dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione; 4.5.2016 L 119/59 Gazzetta ufficiale dell'Unione europea IT (1)Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30). b) si sono impegnati a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63; c) hanno istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati; d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e e) hanno dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi.
3. L'accreditamento degli organi di certificazione di cui ai paragrafi 1 e 2 del presente articolo ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63. In caso di accreditamento ai sensi del paragrafo 1, lettera b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione.
4. Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.
5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.
6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i

Uno strumento certificatorio già operativo, che può essere un ottimo modello per le future esperienze europee, anche se non soggetto ad un meccanismo stringente di accreditamento come richiesto dal GDPR, è "la privacy by design certification" del Privacy and Big Data Institute della Ryerson University, diretto dal 2014 da Ann Cavoukian[53]. L'istituto canadese ha sviluppato uno strumento molto innovativo grazie alla collaborazione con una società del gruppo Deloitte, che si occupa a livello mondiale di consulenza e di analisi dei rischi[54].

La "privacy by design certification" è la prima certificazione basata sulla pbd ed è stata progettata sulla base dei sette principi fondativi di Ann Cavoukian; su queste basi, sono stati sviluppati ben 29 *measurable privacy criteria* e 109 *illustrative privacy controls,* tenendo conto dei requisiti chiave delle legislazioni e degli standard nazionali e internazionali e utilizzando un approccio interdisciplinare[55]. L'obiettivo manifesto è di fornire uno strumento

---

meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.
7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1.
9. La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2".

[53] A tal proposito per ogni informazione si veda il sito di riferimento: < http://www.ryerson.ca/pbdi/privacy-by-design/certification/>.

[54] Si veda il sito del brand, in Rete, <https://www2.deloitte.com/ca/en/pages/about-deloitte/articles/about-deloitte.html?icid=bottom_about-deloitte>: "*Deloitte is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax, and related services to select clients. These firms are members of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). Each DTTL member firm provides services in particular geographic areas and is subject to the laws and professional regulations of the particular country or countries in which it operates*".

[55] A. CAVOUKIAN, *Privacy by Design Certification Program*, Privacy and Big Data Institute at Ryerson University, 2016, available at: <http://www.ryerson.ca/pbdi/privacy-by-design/certification/>, 3: "*Our Privacy by Design Certification is the first of its kind privacy certification that is based on Privacy by Design, a revolutionary privacy framework that has been recognized globally and translated into 37 languages. We then marry this approach by partnering with the expertise of Deloitte, whose global data protection and privacy practice is comprised of multi-disciplinary professionals specializing in technology, policy, security, law, information governance and management, project management, communications, and privacy regulatory affairs. Deloitte operationalized the 7 Foundational Principles by developing 29 measurable privacy criteria and 109 illustrative privacy controls using a unique scorecard approach that aligns to Privacy by Design. The criteria and controls are based on key requirements derived from national and international privacy regulations and best practices*".

che possa avvantaggiare le imprese a livello competitivo e che questo beneficio possa perdurare nel tempo[56].

Il processo di certificazione si compone di tre fasi:

1. Applicazione: le società devono compilare un'applicazione online sul sito del Privacy an Big Data Institute della Ryerson University;
2. Valutazione: il team di esperti di Deloitte valuta i prodotti e i servizi della società attraverso i vari criteri formalizzati. Viene condotta un'analisi sulle pratiche adottate dal soggetto commerciale in materia di privacy, considerando i principi riconosciuti a livello internazionale, tra cui i FIPs, le Linee Guida dell'OECD, e i requisiti richiesti dal quadro normativo nazionale e internazionale che risultano ampiamente armonizzati in più ordinamenti giuridici;
3. Certificazione: se la società soddisfa tutti i requisiti e i criteri, l'attestazione viene infine rilasciata[57].

La certificazione attribuisce alle società la possibilità di svolgere un'attività conforme alla normativa, minimizzando il rischio che invece non sia adeguata, consente di ridurre la probabilità delle contravvenzioni e delle multe, comprese le perdite finanziarie dovute alle violazioni della privacy; fornisce uno strumento utile per aumentare l'affidamento e la fiducia del consumatore e così ottenere sostanziali vantaggi a livello competitivo o riacquistarli dopo gli incidenti e permette alle società di mantenere le migliori pratiche grazie ad una valutazione terza ed imparziale[58].

---

[56] *Ibidem*, 3: "*Most impressive, when you earn Privacy by Design Certification from the Privacy and Big Data Institute at Ryerson, you'll be raising the bar and meeting a privacy standard that is now recognized in more than 35 countries. Doing so will enable you to gain a competitive advantage over other organizations, which is sustainable over time*".

[57] *Ibidem*, 6: "*Step 1, Apply: Applications for certification may be initiated by applying online via Ryerson's website. (ryerson.ca/pbd/certification)*
Step 2, Assess: Using a set of well-defined assessment criteria, Deloitte's privacy and security professionals will test your product, service or offering against the 7 Foundational Principles of Privacy by Design. An assessment of the strength of your privacy practices will be conducted, following internationally-recognized privacy principles, including privacy regulations, industry self-regulatory requirements and industry best practices (e.g., FIPs, OECD, GAPP, CBR and APEC Privacy Framework) using an assessment methodology based on harmonized privacy and security requirements. Taking a holistic and risk-based approach, Deloitte will test your controls using a quantifiable scorecard.
Step 3, Certify: Upon review of the assessment report, certification will be granted only when Ryerson is satisfied that no significant gaps exist as identified by Deloitte in the Privacy Scorecard".

[58] A. CAVOUKIAN, S. KINGSMILL, *Privacy by Design Setting a new standard for privacy certification*, Deloitte and Ryerson University, 2016, available at: < https://www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html#>, 3: "*Privacy by Design certification will give your organization the ability to: Ensure compliance by getting ahead of the legislative curve and minimizing compliance risk; Reduce the likelihood of fines and penalties, including financial losses and/or liability associated with privacy breaches; Build your brand by fostering greater consumer confidence and trust thereby gaining a sustainable competitive advantage; Better manage post-breach incidents to regain consumer trust and*

Nel dettaglio, la valutazione inizia con l'identificazione dello scopo della richiesta di revisione delle pratiche sulla privacy, che può riguardare ogni tipologia di dato raccolti e di processi commerciali o una parte specifica dell'organizzazione, un singolo progetto o sistema sviluppato[59]. Insomma, la certificazione può essere complessiva o mirata ad un particolare prodotto o servizio.

Successivamente, si procede con una verifica sul campo, scegliendo dei campioni di prodotti o servizi e elaborando una tabella per stimare i controlli effettuati sul design e sulle pratiche adottate per la gestione delle informazioni raccolte. Vengono anche effettuate delle interviste all'interno della società, delle visite nelle loro sedi, qualora sia necessario, e un'analisi dei documenti interni per identificare con precisione le questioni legate alla raccolta dei dati. Si valuta se sono presenti adeguati controlli per la protezione della privacy e della sicurezza e se le attività e i controlli sono stati correttamente progettati; in più, si effettua una comparazione tra le soluzioni tecniche ed organizzative adottate e quelle adottabili[60]. In via esemplificativa, per verificare l'adozione del terzo principio fondativo, "*privacy embedded into design*", sono stati predisposti tre criteri chiave e sei procedure di controllo, di cui si riporta una tabella elaborata sulla base del programma di certificazione pubblicato dall'Istituto[61]:

Consideration of Privacy in Design, Documentation Privacy is considered during the technical/solution design	*- Technical design documents, architectural documents, or solution design documents show that privacy was a requirement at the design stage.* *- Privacy of personal information was considered throughout the full life-cycle, from inception through to destruction.*

confidence; Maintain best practices by seeking independent testing of privacy and security controls rather than more self- reporting or testing".

[59] *Ibidem,* 6: "*We begin by working with you to identify the scope of your privacy review. The scope of your assessment can include: All types of personal information holdings and related business processes, including medical and employee information; A defined part of the organization, line of business, function, system, or initiative*".

[60] *Ibidem,* 6: "*Our privacy and security professionals: Use a combination of manual reviews, sampling, and scorecard metrics to assess your current design controls and related information-handling practices; Conduct company interviews, on-site visits (where required), and data discovery (where requested) to identify data collection and residency issues; Evaluate whether a privacy or security control exists, and whether the privacy activities or controls have been properly designed; Compare your solution architecture, related information-handling practices, and operational processes against control activities*".

[61] PRIVACY AND BIG DATA INSTITUTE AT RYERSON UNIVERSITY, DELOITTE, *Privacy by Design Certification Program: Assessment Control Framework*, 2016, available at: < http://www.ryerson.ca/pbdi/privacy-by-design/certification/>, 11.

	- Scalability requirements were considered to ensure privacy is maintained within the foreseeable volume of records held or processed. *- Privacy requirements were determined as part of the business continuity and/or disaster recovery planning and management process, to ensure privacy continuity during adverse situations (e.g. crisis or disaster).*
Privacy in Operational Procedures and Processes Privacy is considered in the design of operational procedures and processes.	*Technical design documents, architectural documents, or solution design documents show that privacy was maintained in the final solution or product, together with any subsequent operational procedures.*
Privacy in Change Management, Privacy is considered in Change Management.	*There is evidence that privacy considerations are appropriately included as part of the change management system and that resulting recommendations are implemented.*

Tutti i risultati dell'indagine sui vari criteri e controlli vengono riportati in un report molto dettagliato, attraverso uno schema per punti, il quale fornisce altresì le indicazioni per colmare le lacune e sviluppare soluzioni più efficaci: l'analisi della certificazione è il mezzo più efficace e appropriato per conoscere e comprendere fino in fondo le pratiche commerciali, le misure tecniche e organizzative dell'impresa, l'eventuale e l'auspicata sua conformità a normativa[62].

Infine, la certificazione viene rilasciata quando tutte le soluzioni indicate sono state adottate e viene attribuito il marchio "Privacy by Design Certification", che appare come una coccarda gialla con la scritta "certified PbyD Ryerson University", da apporre sul sito della società o sui prodotti e

[62] *Ibidem,* 6: "*We deliver results in a restricted use, detailed Privacy Scorecard report that: Identifies any deficiencies or gaps in information system design, policies, and practices; Includes an analysis of personal information and related privacy gaps across the data lifecycle; Contains an analysis of your compliance requirements with all relevant policies, practices, laws, codes, and contracts; Analyzes each element of your organization's privacy program, policies, and procedures; Includes a gap analysis that highlights the gap between your desired state of risk management and the current "as-is" state; Provides detailed observations and recommendations to management for closing identified privacy gaps*".

servizi offerti[63]. Il nove marzo 2016 è stata assegnata la prima certificazione alla Canadian National Insurance Crime Services (CANATICS), per un programma di analisi delle frodi[64].

La validità della certificazione ha durata triennale, ma subisce un processo di rinnovo annuale, soggetto agli eventuali cambiamenti verificatesi all'interno della società e al pagamento di un contributo[65].

Lo strumento certificatorio presentato riproduce appieno il principio di privacy by design e potrebbe essere un buon modello da sperimentare anche nell'Unione Europea. Certamente il costo di un'analisi così approfondita non sarà di poco conto, ma le società dovranno compiere un'inevitabile bilanciamento di interessi. Non si dimentichi che la pbd può rappresentare un ottimo investimento per le aziende per accrescere la fiducia del consumatore e così aumentare i propri profitti senza lucrare sulla commercializzazione delle informazioni raccolte.

Si ritiene che la certificazione possa davvero rappresentare il salto di qualità per le società in materia di privacy: la pbd sarebbe un elemento di sicurezza e un perfetto incentivo. Il 25 maggio 2018 è sempre più vicino e, come ha affermato l'informatico Alan Kay, "*the best way to predict the future is to invent it*"[66].

---

[63] *Ibidem,* 7: "*As part of the certification process, Ryerson: Verifies that any gaps identified in your Privacy Scorecard have been addressed and closed; Displays your company's name on its validation page to provide real-time verification that your certification is current and valid. Once you receive certification, you can display your Privacy by Design certification on your website and/or product or offering, and share your assessment results and certification with your business partners*".

[64] Si veda in Rete sul sito ufficiale dell'Istituto: <http://www.ryerson.ca/pbdi/privacy-by-design/certification/CertificationsGranted/>.

[65] Per le informazioni sul rinnovo si veda in Rete, <http://www.ryerson.ca/pbdi/privacy-by-design/certification/process/>: "*Certifications are valid for a three year period, but must be renewed annually. We will remind you well in advance of your anniversary period with all the details on how to keep your certification current. An important part of renewing your certification is an attestation form in which your organization attests that there has been no change which would affect your certification. When Ryerson is satisfied with your attestation and upon payment of the renewal fee, your Privacy by Design Certification is renewed for another year*".

[66] In Rete: <https://it.wikiquote.org/wiki/Alan_Kay>.

Conclusioni

In queste pagine si è dimostrato che i sistemi informatici possono essere conformati al diritto. La soluzione proposta assicura una tutela *ex ante* e potenzia l'efficienza delle regole giuridiche.

La conformazione delle tecnologie al dato giuridico consente un indubbio innalzamento del livello di prevenzione, rendendo lo strumento informatico inadatto alla commissione di attività dannose o vietate.

Un sistema legale integrato che sfrutti la tecnologia e il suo essere strutturata e strutturabile per rendere più efficaci le norme giuridiche può essere utilizzato per risolvere il problema della protezione della privacy nell'era digitale.

L'architettura del codice può essere creata in relazione al quantitativo di privacy che il diritto, attraverso le sue regole, tutela. Non solo: la configurazione della tecnologia può adeguarsi alle particolari scelte della persona interessata, poiché la medesima deve essere considerata al centro, con un'attenzione peculiare alla sua singolare aspirazione di riservatezza.

La protezione dei dati personali fin dalla progettazione è oggi indicata come uno dei principi in materia di trattamento dei dati personali. Ad affermarlo non è più solo un contributo dottrinale, ma una risoluzione internazionale adottata dalle autorità garanti di tutto il mondo, la prassi della Federal Trade Commission e delle Autorità Canadesi e soprattutto una norma giuridica vincolante dell'Unione Europea. Per l'appunto due ordinamenti molto diversi tra di loro, ossia quello europeo e quello statunitense, hanno entrambi considerato la privacy by design nel loro recente quadro normativo, dimostrando di potersi avvicinare in una materia come quella della privacy, in cui le differenze sono sempre state molto profonde.

L'approccio proattivo di privacy by design trasforma il negative-sum tra privacy e sicurezza in un positive-sum, un win/win model che non sacrifica i diritti individuali per proteggere invece la sicurezza collettiva. In più, le violazioni della privacy risultano minimizzate e disincentivate sin dalla progettazione dei prodotti e dei servizi grazie alla predisposizione di adeguate misure tecniche ed organizzative.

Il principio in questione non è una novità per l'ambito tecnologico perché si inserisce all'interno della proposta definita value sensitive design (VSD), la quale aspira a rappresentare i valori umani nello sviluppo della tecnologia, in una modalità orientata ai principi ed onnicomprensiva. I valori di VSD sottesi alla privacy by design sono i Fair Information Practices e così i principi della privacy riconosciuti a livello internazionale.

Per garantire un'applicazione capillare dell'approccio le norme che ne impongono l'applicazione dovrebbero essere vincolanti per i produttori dei sistemi ICT e per tutti i titolari del trattamento dei dati. Le regole dovranno essere chiare e applicabili al maggior numero di situazioni possibili, senza trascurare le particolarità del caso concreto.

Si aspira all'elaborazione di una norma sulla privacy by design condivisa e condivisibile da più ordinamenti giuridici, grazie alla diffusione delle scelte operative in ambito interno e internazionale: nell'era digitale c'è urgenza di assicurare un'effettiva e maggiore protezione dei dati personali a livello mondiale.

Il principio potrebbe anche essere inserito nei contratti e nelle licenze informatiche, tra le varie condizioni sottoscritte dall'utente e altresì essere introdotto nelle policies aziendali o essere garantito da una certificazione apposita attribuita da un organismo esterno ed imparziale.

Una soluzione che incide così tanto nello sviluppo tecnologico certamente comporta dei costi per il mercato e per i vari prodotti, ma è necessario operare un bilanciamento dei vari interessi. Non si mira a limitare l'innovazione e il progresso, ma si aspira ad attribuire al diritto la funzione di guida prudente e controllata dell'era digitale.

La tutela *ex ante* ha il pregio di infondere fiducia nei consumatori e può risultare un buon investimento per le aziende senza la necessità di lucrare sulla commercializzazione delle informazioni raccolte. Quando si considerano le criticità dell'approccio non si deve dimenticare che grazie alla pbd può essere creato un circolo virtuoso composto da una maggiore sensibilità sociale in tema di privacy, un aumento del potere e della tutela giuridica del consumatore e un adeguamento delle imprese a standard più tutelanti.

La privacy by design, si è visto, può essere un mezzo prezioso per la diffusione di una particolare cultura nella società. La responsabilizzazione del soggetto privato induce a riflettere veramente sulla quantità di informazioni che si vogliono condividere con il resto del mondo e quali, invece, si vogliono in realtà tenere per sé.

La privacy by design non potrà essere una soluzione tutti i possibili trattamenti di dati personali, ma può essere presentata come il futuro della loro protezione. La pbd è la migliore opzione oggi disponibile per bilanciare il potenziale trade-off tra privacy e libertà. Iniziano ad essere presenti gli strumenti per trasferire il principio dalla retorica alla realtà, come dimostrano le applicazioni già operative in vari ambiti giuridici.

La privacy by design è un approccio globale che comporta una maggiore tutela dei diritti dei cittadini, in modo coerente e completo. Progettare le tecnologie in modo privacy-friendly è doveroso non solo per proteggere la riservatezza e i dati degli individui, ma anche per garantire che l'esercizio degli altri diritti fondamentali non sia ingiustamente penalizzato.

Il punto di partenza e di arrivo è sempre il diritto e il suo potere di conformare la tecnologia alle sue regole.

Privacy is not dead, be aware of it.

Bibliografia

AGNINO F., *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (vedi contratto FB)*, in *Giur. merito*, 2012, fasc. 12, 2555-2568.

AIELLO G. F., *La protezione dei dati personali dopo il Trattato di Lisbona. Natura e limiti di un diritto fondamentale "disomogeneo" alla luce della nuova proposta di "General Data Protection Regulation"*, in *Oss. Dir. civ. comm.*, 2015, fasc. 2, 421-445.

ATZORIA L., IERAB A., MORABITOC G., *The Internet of Things: a survey*, *Computer Networks* 2787 (2010).

BALDUCCI ROMANO F., *La Protezione dei dati personali nell'Unione Europea tra libertà di circolazione e diritti fondamentali dell'uomo,* in *Riv. it. dir. pubbl. com.*, 2015, fasc. 6, 1619-1659.

BARBAS S., *Saving privacy from history*, 61 *DePaul L. Rev*. 973 (2012).

BELLAVISTA A., *Società della sorveglianza e protezione dei dati personali*, in *Contr. Impr.,* 1996, 63-81.

BENTHAM J. (a cura di FOUCALT M. e PERROT M.), *Panopticum, ovvero la casa d'ispezione*, Marsilio, Venezia, 2002.

BERGADANO F., MANTELERO A., RUFFO G., SARTOR G., *Privacy digitale. Giuristi e informatici a confronto,* Giappichelli, Torino, 2006.

BERNSTEIN G., *When new technologies are still new: windows of opportunity for privacy protection*, 51 *Vill. L. Rev.* 921 (2006).

P. BIRNSTILL, S. BRETTHAUER, S. GREINER, E. KREMPEL, *Privacy-preserving surveillance: an interdisciplinary approach*, 5 *IDPL* (2015).

BLUME P., *It is time for tomorrow: EU data protection reform and the Internet*, 18 *JIL* 3 (2015).

BONA C., RUMIATI R., *Psicologia cognitiva per il diritto*, Bologna, Il Mulino, 2013.

BOURDILLON S. S., *Privacy vs security… Are we done yet?,* in S. S. BOURDILLON, J. PHILLIPS, M. D. RYAN (a cura di), *Privacy vs Security*, Springer, 2014, 1.

CANEPA G., *Criminologia e scienze criminali. Un approccio interdisciplinare nella prospettiva medico-legale, in Riv. It. med. Leg.,* 1990, fasc. 2, pt. 1, 387-400.

CASO R., *Digital Rights Management - Il commercio delle informazioni digitali tra contratto e diritto d'autore,* Ristampa digitale, Trento, 2006, in Rete: <eprints.biblio.unitn.it/4375/1/Roberto.Caso_DRM.pdf>.

CASO R., *La Corte di giustizia e la tutela delle misure tecnologiche di protezione del diritto d'autore: cinquanta (e più) sfumature di grigio*, Nota a CGUE sez. IV 23 gennaio 2014 (causa C-355/12), in *Foro it.*, 2014, fasc. 4, 207-210.

CAVOUKIAN A., *Guidelines for the use of video surveillance cameras in public places,* Information & Privacy Commissioner, Ontario, Canada, 2007, available at: <http://www.ontla.on.ca/library/repository/mon/20000/277889.pdf>.

CAVOUKIAN A., *Privacy and video surveillance in mass transit systems: a special investigation report – Privacy Investigation Report MC07-68*, Information and Privacy Commissioner of Ontario, 2008, available at: <http://www.ontla.on.ca/library/repository/mon/21000/279882.pdf>.

CAVOUKIAN A., *Privacy by design,* Information & Privacy Commissioner, Ontario, Canada, 2009, available at: <www.privacybydesign.ca>.

CAVOUKIAN A., *Privacy by design: the definitive workshop - A foreword by Ann Cavoukian*, 3 *IDIS* 247 (2010).

CAVOUKIAN A., *Operationalizing Privacy by design: a guide to implementing strong privacy practices*, Information and Privacy Commissioner, Ontario, 2012, available at: <www.privacybydesign.ca>.

CAVOUKIAN A., EL EMAM K., et al., *Introducing Privacy-Protective Surveillance: achieving privacy and effective counter-terrorism*, Information and Privacy Commissioner, Ontario, 2013, available at: <www.privacybydesign.ca>.

CAVOUKIAN A., *International council on global privacy and security, by design*, Unintended Consequences of Technology, IEEE Potentials September/October 2016, 43-46.

CAVOUKIAN A., *Privacy by Design Certification Program*, Privacy and Big Data Institute at Ryerson University, 2016, available at: <http://www.ryerson.ca/pbdi/privacy-by-design/certification/>.

CAVOUKIAN A., JONES HARBOUR P., *White paper for regulators, decision-makers, policy-makers*., in A. CAVOUKIAN (a cura di), *Privacy by design, From rhetoric to reality,* Information & Privacy Commissioner, Ontario, Canada, 2011, available at: <www.privacybydesign.ca>.

CAVOUKIAN A., KINGSMILL S., *Privacy by Design Setting a new standard for privacy certification*, Deloitte and Ryerson University, 2016, available at: < https://www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html#>.

CIUSA F., VARGAS-CHAVES I., *Considerazioni critiche nella dottrina giuridica italiana sul DRM*, in *Principia Iuris*, 2013, fasc. 1, 325-340.

COHEN J. E., *DRM and Privacy,* 18 *Berkeley Tech. L.J.* 575 (2003).

COHEN J. E., *What privacy is for,* 126 *Harv. L. Rev*. 1904 (2013).

COLESKY M., HOEPMAN J., HILLEN C., *A critical analysis of privacy design strategies,* Conference Paper, IEEE Security and Privacy Workshops (SPW), 2016.

COSTA L., POULLET Y., *Privacy and the Regulation of 2012*, 28 *CLSR* 254 (2012).

CUNIBERTI M., *Tecnologie digitali e libertà politiche*, in *Dir. informazione e informatica*, 2015, fasc. 2, 275-314.

DE HERT P., PAPAKONSTANTINOU V., *The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals,* 28 *CLSR* 130 (2012).

DE HERT P., *The EU data protection reform and the (forgotten) use of criminal sanctions*, 4 *IDPL* 262 (2014).

DE ROSA V., *La Formazione Di Regole Giuridiche Per Il "Cyberspazio",* in *Dir. informazione e informatica*, 2003, fasc. 2, 361-400.

DENTE B., LUGARESI N., RIGHETTINI M. S. (a cura di), *La politica della privacy tra tutela dei diritti e garanzia dei sistemi*, Passigli, Firenze, 2009.

DEVRIES W. T., *Protecting privacy in the Digital Age*, 18 *Berkeley Tech. L.J.* 283 (2003).

DI RESTA F., *La tutela dei dati personali nella società dell'informazione*, con il contributo di A. BRUN, F. PIZZETTI (a cura di), Giappichelli, Torino, 2009, 81.

DURANTE M., PAGALLO U. (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, UTET giuridica, Torino, 2012.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Privacy and Data Protection by Design – from policy to engineering*, 2014, available at: <www.enisa.europa.eu>.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY, *Privacy by design in big data, an overview of privacy enhancing technologies in the era of big data analytics*, 2015, in Rete: <www.enisa.europa.eu>.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, Council of Europe, *Handbook on European data protection law,* 2014, available at: <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law>.

FACEBOOK IRELAND, "Facebook's Views on EU Data Protection Regulation", March 30 2012, available at: <http://www.europe-v-facebook.org/FOI_Facebook_Lobbying.pdf>

FERRARA SANTAMARIA M., *Il diritto alla illesa intimità privata "right of privacy"*, in *Dir. aut.*, 1996, fasc. 4, 402-404.

FERRARA SANTAMARIA M., *Il diritto dell'illesa intimità privata*, in *Riv. dir. priv.*, 1937, vol. I, 168-191.

FINOCCHIARO G., *La Giurisprudenza della Corte di Giustizia in materia di dati Personali da Google Spain a Schrems*, in *Dir. informazione e informatica*, 2015, fasc. 4-5, 779-799.

FINOCCHIARO G., *Lex mercatoria e commercio elettronico, il diritto applicabile ai contratti conclusi su Internet*, in *Contr. impr.*, 2001, fasc. 2, 571-610.

FINOCCHIARO G., *Riflessioni su Diritto e Tecnica,* in *Dir. informazione e informatica*, 2012, fasc. 4-5, 831-840.

FROSINI V., *Informatica diritto e società*, Giuffré, seconda edizione, Milano, 1992.

GALGANO F., *Dibattito a più voci intorno alla crisi dell'università italiana e al libro di Vincenzo Zeno Zencovich - Ci vuole poco per fare una università migliore. Guardando oltre la "riforma Gelmini",* in *Contr. impr.*, 2012, fasc. 2, 315-338.

GILBERT F., *Proposed EU data protection regulation - issues to consider when planning for the future regime,* 17 *JIL* 1 (2014).

GRANARA D., *Il fronte avanzato del diritto alla riservatezza,* in *Riv. it. dir. pubbl. com.*, 2015, fasc.3-4, 897-915.

GRIMMELMANN J., *Privacy as product safety*, 19 *Widener L.J.* 793 (2010).

GUARDA P., *Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks*, in *Ciberspazio e dir.*, 2008, 65-91.

GUARDA P., ZANNONE N., *Towards the development of Privacy-Aware Systems,* 51 *Info. & Software Tech*. 337 (2009).

GUARDA P., *Fascicolo sanitario elettronico e protezione dei dati personali*, Quaderni dei Dipartimento di Scienze Giuridiche, Trento, 2011.

GÜRSES S., TRONCOSO C., DIAZ C., *Engineering Privacy by Design*, Conference on Computers Privacy Data Protection 317 (2011).

HARTZOG W., *Reexamining privacy value: the value of modest privacy protections in a hyper social world,* 12 *Colo. Tech. L.J.* 333 (2014).

HARTZOG W., STUTZMAN F. D., *Obscurity by Design*, 88 *Wash. L. Rev.* 385 (2013).

HASTY A., *Treating consumer data like oil: how re-framing digital interactions might bolster the federal trade commission's new privacy framework*, 67 *Fed. Comm. L.J.* 293 (2014-2015), 323.

HOOFNAGLE C. J., *Federal Trade Commission Privacy Law and Policy*, UC Berkeley Public Law Research Paper No. 2800276, Cambridge University

Press, 2016, available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800276> .

HOOFNAGLE C. J., *Assessing the Federal Trade Commission's Privacy Assessments*, 14(2) *IEEE Security & Privacy* 58 (2016), available at: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163>.

HUSTINX P., *Privacy by design: delivering the promises,* 3 *IDIS* 253 (2010).

KHAN F., *Survey of Recent FTC Privacy Developments and Enforcement*, 67 Bus. Law. 297 (2011).

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, HEWLETT-PACKARD (HP), *RFID and Privacy Guidance for Health-Care Providers*, 2008, available at: < http://www.ontla.on.ca/library/repository/mon/20000/279038.pdf>.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, INTEL, GE HEALTHCARE, *Remote Home Health Care Technologies: How to Ensure Privacy? Build It In: Privacy by Design***,** 2009, available at: < http://www.ontla.on.ca/library/repository/mon/23011/296578.pdf>.

IRTI N.*, La filosofia di una generazione,* in *Contr. impr.*, 2011, fasc. 6, 1295-310.

IRTI N., *Norma e luoghi: problemi di geo-diritto*, Laterza, Bari, 2006.

IRTI N., SEVERINO E.*, Le domande del giurista e le risposte del filosofo (un dialogo su diritto e tecnica),* in *Contr. impr.,* 2000, fasc. 2, 665-679.

ISLAM M. B., IANNELLA R., *Privacy by Design: Does it matter for social networks?*, IFIP Summer School 2011, International Federation for Information Processing, University of Trento, available at: <http://eprints.qut.edu.au/60607/>.

JAMMET A., *The evolution of EU law on the protection of personal data,* 3 *European (Legal) Studies on-line papers, Queen's University Belfast - School of Law* 1 (2014).

JENNINGS M., *To track or not to track: recent legislative proposals to protect consumer privacy*, 49 *Harv. J. on Legis*. 193 (2012).

JUTLA D. N., *Layering privacy on operating systems, social networks, and other platforms by design,* 3 *IDIS* 319 (2010).

KIANIEFF M., *The evolution of consumer privacy law: how privacy by design can benefit from insights in commercial law and standardization*, 10 *CJLT* 1 (2012).

KLITOU D., *Privacy-Invading Technologies and Privacy by Design, safeguarding privacy, liberty and security in the 21st century*, T.M.C. Asser Press, 25 Information Technology and Law Series, Hague (2014).

KOOPS B. J., LEENES R., *Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law*, 28 *Int. Rev. Law Comput. Tech.* 1 (2013).

KREBS D., *"Privacy by Design": nice-to-have or a necessary principle of data protection law?,* 4 *JIPITEC* 2190 (2013).

LADINSKY J., *The teaching of law and social science courses in the United States*, in *Sociologia dir.*, 1976, fasc. 1, 51-70.

LAUKYTE M., *An interdisciplinary approach to Multi-agent Systems: bridging the gap between law and computer science,* in *Informatica e dir.*, 2013, fasc. 1, 223-241.

LEDERER S. et al., *Personal privacy through understanding and action: five pitfalls for designers*, 8 *Pers. & Ubiquitous Computing* 440 (2004).

A. LEVIN, M. J. NICHOLSON, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 *U. Ottawa L. & Tech. J.* 357 (2005).

LESSIG L., *Code and Other Laws of Cyberspace*, Basic Books, A Member of the Perseus Books Group, New York, 1999.

LESSIG L., *Code*, *version 2.0*, Basic Books, A Member of the Perseus Books Group, New York, 2006.

LEVIN A., NICHOLSON M. J., *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 *U. OTTAWA L. & TECH. J.* 357 (2005).

LUGARESI N., *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffré, Milano, 2000.

MANTELERO A., *Privacy*, in *Contr. impr.*, 2008, fasc. 3, 757-779.

MANTELERO A., *Regole tecniche e giuridiche: interazioni e sinergie nella disciplina di internet*, in *Contr. impr.*, 2005, fasc. 2, 658-686.

MANTELERO A., *Riforma della direttiva comunitaria sulla Data Protection e Privacy Impact Assessment, Verso una maggiore responsabilità dell'autore del trattamento?,* in *Dir. informazione e informatica*, 2012, fasc. 1, 145-153.

MASSEY A., *Why understanding technology is essential for privacy law*, 51 *Idaho L. Rev.* 695 (2015).

MAZZEO M., *Privacy: finisce l'era del D.P.S.*, in *Obbl. Contr*., 2008, fasc. 8-9, in Leggi d'Italia.

MENGONI L., *Diritto e tecnica,* in *Riv. trim. dir. proc. civ.,* 2001, fasc. 2, 1-10.

MONTALDO S., *Internet e commons: le risorse della rete nella prospettiva dei beni comuni,* in *Dir. informazione e informatica*, 2013, fasc. 2, 287-306.

MULLIGAN D. K., KING J., *Bridging the gap between privacy and design*, 14 *U. Pa. J. Const. L.* 989 (2012).

ORWELL G. (a cura di RUSSO L.), *1984*, Aesthetica edizioni, Palermo, 1986.

PAGALLO U., *La tutela della privacy negli Stai Uniti d'America e in Europa, modelli giuridici a confronto,* Giuffrè, Milano, 2008.

PALMIERI A., *DRM e disciplina europea della protezione dei dati personali* in R. CASO (a cura di), *Digital Rights Management: problemi teorici e prospettive applicative: atti del Convegno tenuto presso la Facoltà di Giurisprudenza di Trento il 21 ed il 22 marzo 2007,* Quaderni del dipartimento di Scienze Giuridiche, n. 70, Trento, 2008.

PASCUZZI G., *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica*, Zanichelli, Bologna, 2013.

PASCUZZI G. (a cura di), *Il diritto dell'era digitale*, Il Mulino, Bologna, 2016.

PELLEGRINO G., *I rischi del diritto nella Rete globale*, in *Informatica dir.*, 2009, fasc. 1, 255-267.

PRINCIPATO A., *Verso nuovi approcci alla tutela della privacy: privacy by design e by default settings*, in *Contr. impr. Europa,* 2015, fasc. 1, 197-229.

PRIVACY AND BIG DATA INSTITUTE AT RYERSON UNIVERSITY, DELOITTE, *Privacy by Design Certification Program: Assessment Control Framework*, 2016, available at: <http://www.ryerson.ca/pbdi/privacy-by-design/certification/>.

RABAZZI C., *Regole sulla sicurezza dei dati nel recente "codice sulla privacy",* in *Ciberspazio e dir*., 2003, fasc. 3-4, 331-351.

RAMIREZ E., *Privacy by Design and the New Privacy Framework of the U.S. Federal Trade Commission,* Remarks of Commissioner in the *Privacy by Design Conference*, Hong Kong, June 13, 2012.

REDING V., *The European data protection framework for the twenty-first century,* 2 *IDPL* 119 (2012).

REIDENBERG J. R., *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 *Tex. L. Rev.* (1997-1998).

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. Informazione e Informatica*, 2015, fasc.4-5, 697.

RODOTÀ S., *Diritto, scienza, tecnologia: modelli e scelte di regolamentazione*, in *Riv. crit. dir. priv.*, 2004, fasc. 3, 357-375.

RODOTÀ S., *Il diritto di avere diritti*, Laterza, Bari, 2012.

RODOTÀ S., *Intervista su privacy e libertà*, (a cura di) P. CONTI, Laterza, Bari, 2005.

ROSSELLO C., *Commercio Elettronico: la governance di internet tra diritto statuale, autodisciplina, soft law e lex mercatoria*, Giuffré, Milano, 2006.

ROTENBERG M., JACOBS D., *Updating the law of information privacy: the new framework of the European Union*, 36 *Harvard JLPP* 606 (2013).

RUBINSTEIN I. S., GOOD N., *Privacy by design: a counterfactual analysis of Google and Facebook privacy incidents*, 28 *Berkeley Tech. L.J.* 1333 (2013).

RUBINSTEIN I. S., *Regulating privacy by design*, 26 *Berkeley Tech. L.J.* 1409 (2011).

SACCO R., *Introduzione al diritto comparato,* Utet, Torino, 2011.

SARTOR, G., *Il diritto della rete globale*, in *Ciberspazio e dir.*, 2003, fasc. 1, 67-94.

SCHAAR P., *Privacy by Design*, 3 *IDIS* 267 (2010).

SCHARTUM D. W., *Making privacy by design operative*, 24 *IJLT* 151 (2016).

SCHIRA A., *Protecting Progress and Privacy: The Challenges of Smart Grid Implementation*, 6 *ISJLP* 629 (2011).

SCHERMER B. V., *Surveillance and privacy in the ubiquitous network society*, 1 *Amsterdam L.F.* 63 (2008-2009).

SCHWARTZ P. M., *Property, Privacy, and Personal Data,* 117 *Harv. L. Rev.* 2055 (2004).

SOLOVE D. J., *Conceptualizing privacy*, 90 *Cal. L. Rev.* 1087 (2002).

SOLOVE D. J., A taxonomy of privacy, 154 U. Pa. L. Rev. 477 (2006).

SOLOVE D. J., HARTZOG W., *The FTC and the new common law of privacy*, 114 *Colum. L. Rev.* 583 (2014).

SOLOVE D. J., *Nothing to Hide: the false tradeoff between privacy and security, Introduction*, Yale University Press, New Haven, 2011.

SOLOVE D. J., SCHWARTZ P. M., *Reconciling Personal Information in the United States and European Union*, 102 *Cal. L. Rev.* 877 (2014).

SOLOVE D. J., *Understanding Privacy, Introduction,* Harvard University Press, Boston, 2008.

SPEDICATO G., *Le misure tecnologiche di protezione del diritto d'autore nella normativa italiana e comunitaria*, in *Ciberspazio e dir.*, 2006, fasc. 4, 535-580.

SPEDICATO G., *Law as Code? Divertissement sulla lex informatica,* in *Ciberspazio e dir.*, 2009, fasc. 2, 233-259.

TIEN L., *Architectural regulation and the evolution of social norms*, 7 *Yale J. L. & Tech.* 1 (2004).

TENE O., *New harm matrix for cybersecurity surveillance*,12 *Colo. Tech. L.J.* 391 (2014).

VICTOR J. M., *The EU General Data Protection Regulation: toward a property regime for protecting data privacy*, 123 *Yale L.J.* 513 (2013).

WALDMAN A. E., *Privacy, Sharing, and Trust: The Facebook Study,* 67 *Case Western Reserve L. Rev.* 1 (2017).

WARREN S. D., BRANDEIS L. D., *The Right to Privacy*, 4 *Harv. L. Rev.* 193 (1890).

ZENCOVICH V. Z., *Una lettura comparatistica della L. n. 675/96 sul trattamento dei dati personali,* in *Riv. trim. dir. proc. civ.*, 1998, fasc. 3, 733.

ZENCOVICH V. Z., *I diritti della personalità*, in N. LIPARI, P. RESCIGNO (a cura di), *Diritto civile*, vol. 1, Giuffré, 2009, 495-554.

Fonti normative

<u>Unione Europea</u>

Direttiva n. 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla "tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

Art. 8 Carta dei Diritti Fondamentali dell'Unione Europea, (2000/C 364/01).

Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativa al "trattamento dei dati personali e sulla tutela della vita privata nel settore delle comunicazioni elettroniche".

Versione consolidata del Trattato sull'Unione europea e Trattato sul funzionamento dell'Unione europea, Gazzetta Ufficiale n. C 326 del 26/10/2012.

Proposal for a Regulation of the European Parliament and of The Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25 January 2012.

Regolamento (UE) n. 1024/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relativo alla "cooperazione amministrativa attraverso il sistema

di informazione del mercato interno e che abroga la decisione 2008/49/CE della Commissione («regolamento IMI»)".

Regolamento (Ue) del Parlamento Europeo e del Consiglio del 21 maggio 2013 n. 524 relativo alla "risoluzione delle controversie online dei consumatori e che modifica il regolamento (CE) n. 2006/2004 e la direttiva 2009/22/CE (regolamento sull'ODR per i consumatori)".

Decisione del Consiglio del 3 dicembre 2013 N. 743 che stabilisce il programma specifico di attuazione del programma quadro di ricerca e innovazione (2014-2020) – Orizzonte 2020 e abroga le decisioni 2006/971/CE, 2006/972/CE, 2006/973/CE, 2006/974/CE e 2006/975/CE.

Regolamento (Ue) del Parlamento Europeo e del Consiglio del 23 luglio 2014 n. 910 in materia di "identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE".

Decisione Ue del Parlamento Europeo e del Consiglio del 15 maggio 2014 n. 554 relativa alla "partecipazione dell'Unione al programma di ricerca e sviluppo a sostegno di una vita attiva e autonoma avviato congiuntamente da più Stati membri".

Reg. 27 aprile 2016, n. 2016/679: Regolamento del Parlamento Europeo relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati").

Direttiva 2016/1148 del Parlamento Europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

Canada e Stati Uniti

U.S. Department of Health, Education & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, *Records Computers and the Rights of citizens*, 1973.

The Commercial Privacy Bill of Rights Bill of 2011, available at: <https://www.congress.gov/bill/112th-congress/senate-bill/799/text>.

Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11, available at <http://laws-lois.justice.gc.ca/eng/const/page-15.html#h-39>.

Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), available at: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>.

Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, available at: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html>.

Italia

Legge 20-05-1970, n. 300 Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento in G.U. n. 131 del 27-05-1970, in Rete: <http://normattiva.it/>.

Legge 31 dicembre 1996 n. 675, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali.

Bolzano - Provincia autonoma Delib. G. P. 26/07/2016, n. 846, Approvazione del Regolamento per l'utilizzo del sistema integrato di videosorveglianza degli uffici centrali della Provincia autonoma di Bolzano, pubblicata nel B.U. Trentino-Alto Adige 2 agosto 2016, n. 31.

Gruppo art. 29 – Garanti e altre Autorità Europee

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, Raccomandazione 4/99 concernente l'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali adottata, 5143/99/IT/def. WP 26 adottata il 7 settembre 1999.

Article 29 Data Protection Working Party, Working document on data protection issues related to intellectual property rights, WP 104 05/EN.

Gruppo di lavoro articolo 29 per la protezione dei dati personali, 01248/07/IT, WP 136, Parere 4/2007 sul concetto di dati personali, adottato il 20 giugno 2007.

Garante per la protezione dei dati personali, Semplificazione delle misure di sicurezza contenute nel disciplinare tecnico di cui all'Allegato B) al Codice in materia di protezione dei dati personali - 27 novembre 2008 G.U. n. 287 del 9 dicembre 2008.

Garante per la Protezione dei Data Personali, Linee Guida in tema di Fascicolo Sanitario elettronico e di dossier sanitario del 16 luglio 2009 in G.U. n. 178 03-08-2009.

Article 29 Data Protection Working Party, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, WP 168 02356/09/EN.

Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy del 18.3.2010.

Gruppo Di Lavoro Per La Tutela Dei Dati Ex Art. 29, Parere 1/2010 sui concetti di "responsabile del trattamento" e "incaricato del trattamento", adottato il 16 febbraio 2010.

International Working Group on Data Protection in Telecommunications, Privacy by Design and Smart Metering: Minimize Personal Information to Maintain Privacy (2011), available at: <http://www.datenschutz-berlin.de/attachments/842/675.43.18_WP_Privacy_and_Smart_ Metering.pdf>.

Art 29 Working Party, Opinion 12/2011 on smart metering, WP 183 (2011)., available at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf>.

Garante per la Protezione dei Dati Personali, Parere 26/03/2015, n. 3898704, “Avvio della consultazione pubblica su Internet delle cose (Internet of Things)”.

Report on the 2010 Office of the Privacy Commissioner of Canada’s, Consultations on Online Tracking, Profiling and Targeting, and Cloud

Computing, available at <https://www.priv.gc.ca/media/1961/report_201105_e.pdf>

Office of the privacy Commissioner of Canada, OPC, Interpretation Bulletin: Safeguards, 2015 available at: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/>.

Garante per la Protezione dei Dati Personali, Verifica preliminare - Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze dell'8 settembre 2016, doc. web n. 5497522, in Rete: < http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5497522>.

Soft law

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, in the form of a Recommendation by the Council of the OECD, 23 september 1980.

Commissione Europea, Tecnologie di rafforzamento della tutela della vita privata (PET), Il quadro giuridico vigente, MEMO/07/159, Bruxelles, 2 maggio 2007.

Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Sulla promozione della protezione dei dati mediante tecnologie di rafforzamento della tutela della vita privata (PET), COM (2007) 228.

Consiglio Europeo, Programma di Stoccolma - un'Europa aperta e sicura al servizio e a tutela dei cittadini, (2010/C 115/01).

32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, Jerusalem, Israel 27-29 October, 2010.

Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni "un'agenda digitale europea", COM (2010) 245.

Comunicazione della Commissione al Parlamento Europeo e al Consiglio, Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia, COM (2010) 385.

Federal Trade Commission, Recommendations for Businesses and Policymakers, Protecting consumer privacy in an era of rapid change, 2012.

Comunicazione della Commissione al Parlamento Europeo, al Consiglio e al Comitato Economico e Sociale Europeo, "Politica industriale della sicurezza, Piano d'azione per un'industria della sicurezza innovativa e competitiva", COM (2012) 417.

OECD, The OECD Privacy Framework, 2013.

Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato Delle Regioni, "Agenda europea sulla sicurezza", COM (2015) 185.

Comunicazione della Commissione al Parlamento Europeo e al Consiglio, "Sistemi d'informazione più solidi e intelligenti per le frontiere e la sicurezza", COM (2016) 205.

Fonti giurisprudenziali

Cass., Sez. I civile, 22 dicembre 1956 n. 4487, in *Foro It.* 1957, vol. 80, 4-11 e nota a sentenza dell'Avv. A. DE CUPIS, 232-234 nello stesso tomo.

Cass., Sez. I civile, 20 aprile 1963 n. 990, in *Foro It.* 1963, vol. 86, 877-879 e nota a sentenza dell'Avv. A. DE CUPIS, 1298-1300 nello stesso tomo.

Cass., Sez. I civile, 27 maggio 1975 n. 2129, in *Foro It.* 1976, vol. 99, 2895-2907.

Tribunale Nola, sez. II, 03/02/2009, in De Iure: <https://www.iusexplorer.it/Dejure/Sentenze?idDocMaster=1998300&idDataBanks=6&idUnitaDoc=0&nVigUnitaDoc=1&pagina=0&NavId=514469624&pid=19>.

Tribunale Bari, 11/01/2016, n. 73, in De Iure: <https://www.iusexplorer.it/Dejure/Sentenze?idDocMaster=4901195&idDataBanks=6&idUnitaDoc=0&nVigUnitaDoc=1&pagina=0&NavId=526920785&pid=19>.

Controversie delle agenzie ed autorità

Hunter v. Southam, 2 S.C.R. 145, 159-60 (1984).

Federal Trade Commission v. Frostwire LLC and Angel Leon, United States District Court Southern District of Florida, Case No. 11-23643-CV-GRAHAM.

Federal Trade Commission, Complaint for Permanent Injunction and Other Equitable Relief, Federal Trade Commission v. Frostwire LLC and Angel Leon.

Federal Trade Commission v. Wyndham Worldwide Corporation, et al., United States District Court for The District of New Jersey, Civil Action No. 13-1887 (ES), 2014 U.S. Dist. LEXIS 84913.

Office of the Privacy Commissioner of Canada, PIPEDA Case Summary #2011-001, Google Inc.

Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2013-001 Investigation into the personal information handling practices of WhatsApp Inc.

Sitografia

http://www.wordreference.com/: sito web che fornisce gratuitamente un utilissimo dizionario bilingue per le traduzioni dall'inglese.

http://dictionary.cambridge.org/it/: portale online dell'omonimo dizionario cartaceo monolingua inglese della Cambridge University Press.

https://www.ssrn.com/en/: portale scientifico che fornisce moltissimi articoli di riviste o capitoli di libri pubblicati in open access.

http://normattiva.it/: portale italiano che fornisce i testi della legge italiana vigente.

http://hls.harvard.edu/dept/academics/programs-of-study/law-science-and-technology/: fornisce le informazioni sul corso "Law, Science, and Technology" all'Harvard Law School.

https://www.law.berkeley.edu/php-programs/courses/coursePage.php?cID=18509&termCode=B&termYear=2017

https://www.justice.gov/opcl/privacy-act-1974: fornisce le informazioni per il corso “Computer Law” alla Berkley Law dell’Università della California.

http://ec.europa.eu/justice/data-protection/reform/index_en.htm: portale sulle riforme dell’Unione Europea per la protezione dei dati personali.

http://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali: fornisce la definizione di dato personale adottata dal Garante Italiano per la Protezione dei Dati Personali.

http://eur-lex.europa.eu/procedure/EN/2012_11: fornisce le informazioni sulla Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5035744: fornisce il comunicato stampa del Garante per la Protezione dei Dati Personali del 24 maggio 2016 in merito all’entrata in vigore del GDPR.

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718: fornisce il comunicato stampa del Garante per la Protezione dei Dati Personali del 4 maggio 2016 in merito alla pubblicazione sulla Gazzetta Ufficiale UE del Pacchetto protezione dati del 2016.

http://www.lastampa.it/2016/07/31/esteri/il-garante-ue-inutile-limitare-la-privacy-prima-deve-migliorare-lantiterrorismo-j3JYDCwI0VPJWGymWDhLmI/pagina.html: articolo de La Stampa intitolato “Il Garante Ue: inutile limitare la privacy, prima deve migliorare l’antiterrorismo - Buttarelli: “Una volta quando non si voleva affrontare un problema si creava una commissione d’inchiesta, adesso si istituisce una nuova banca dati”, contenente un’intervista al Garante Europeo per la Protezione dei Dati in merito al rapporto tra privacy e sicurezza.

http://www.lastampa.it/2016/08/01/italia/cronache/il-garante-della-privacy-soro-i-controlli-di-massa-inefficaci-necessario-selezionare-i-bersagli-xxnC4MO5XBHENIurp4EalL/pagina.html: articolo de La Stampa intitolato “Il Garante della privacy Soro: “I controlli di massa inefficaci, necessario selezionare i bersagli”, al Garante Italiano sulla sicurezza dei dati personali in Italia.

https://ec.europa.eu/digital-single-market/en/glossary#letter_p: portale che fornisce il Glossario dell'Unione Europea, contente anche la definizione di privacy by design.

https://icdppc.org/the-conference-and-executive-committee/strategic-direction-mission-and-vision/: fornisce le informazioni sugli obiettivi dell'International Conference of Data Protection and Privacy Commissioner.

https://icdppc.org/document-archive/rules-procedures/: fornisce le informazioni sulle regole procedurali dell'International Conference of Data Protection and Privacy Commissioner.

http://www.coe.int/it/web/portal/home: sito web ufficiale del Consiglio d'Europa.

http://eur-lex.europa.eu/: portale di accesso alle norme dell'Unione Europea.

http://europa.eu/rapid/press-release_SPEECH-10-16_it.htm: fornisce il discorso al Data Protection Day di Viviane Reding, Member of the European Commission responsible for Information Society and Media del 28 gennaio 2010.

http://ec.europa.eu/internal_market/imi-net/library/index_it.htm#maincontentSec3: fornisce la documentazione di riferimento per il programma europeo IMI.

https://webgate.ec.europa.eu/odr/main/?event=main.home.show: sito web ufficiale della piattaforma dell'Online Dispute Resolution.

http://www.horizon2020news.it/: portale italiano in cui vengono forniti gli aggiornamenti sul Programma Quadro europeo per la Ricerca e l'Innovazione (2014 – 2020), Horizon 2020.

http://europa.eu/geninfo/query/index.do: motore di ricerca per i documenti normativi e di soft law dell'Unione Europea.

http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law: portale dell'European Union Agency for Fundamental Rights contenente i riferimenti all'Handbook on European data protection law del 2014.

https://secure.edps.europa.eu/EDPSWEB/edps/EDPS: sito web ufficiale dell'European Data Protection Supervisor.

https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm: portale dell'OECD che fornisce le Guidelines on the Protection of Privacy and Transborder Flows of Personal Data e le informazioni ad esse collegate.

https://www.ftc.gov/: sito web ufficiale della Federal Trade Commission.

https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority: fornisce le informazioni sull'enforcement della Federal Trade Commission.

https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation: fornisce tutta la documentazione del caso Federal Trade Commission v. Wyndham Worldwide Corporation.

https://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter: fornisce tutta la documentazione del caso Federal Trade Commission v. Google Inc.

https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon: fornisce tutta la documentazione del caso Federal Trade Commission v. Frostwire LLC and Angel Leon.

http://www.ryerson.ca/pbdi/about/exec_message/: fornisce gli obiettivi e la metodologia del Privacy & Big Data Institute di Toronto nella Provincia dell'Ontario in Canada.

https://www.ipc.on.ca/: sito web Ufficiale dell'Information and Privacy Commissioner dell'Ontario.

http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5274/index.do: fornisce i documenti delle decisioni della Supreme Court of Canada nel caso Hunter et al. v. Southam Inc.

http://laws-lois.justice.gc.ca/eng/const/page-15.html#h-39: portale di Justice Law del Governo del Canada che fornisce il testo aggiornato del Constitution Act del 1982.

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/: portale che fornisce tutti i riferimenti sulla PIPEDA e gli atti ad essa collegati.

http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html: portale di Justice Law del Governo del Canada che fornisce il testo dei Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information.

https://support.google.com/mail/answer/1698228?hl=it: fornisce il comunicato di Google sul ritiro dal mercato di Google Buzz.

https://www.priv.gc.ca/media/1961/report_201105_e.pdf: fornisce il Report on the 2010 Office of the Privacy Commissioner of Canada's, Consultations on Online Tracking, Profiling and Targeting, and Cloud Computing.

http://www.csagroup.org/legal/privacy/csa-group-privacy-statement/: sito web ufficiale del CSA contenente il CSA Model Code for the protection of privacy information.

https://www.priv.gc.ca/en/: sito web ufficiale dell'Office of Privacy Commissioner del Canada.

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/: fornisce i riferimenti per i vari Bollettini Interpretativi dell'OPC sulla PIPEDA.

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_08_sg/: fornisce l'Interpretation Bulletin sulle Safeguards dell'OPC, aggiornato al 2015.

https://www.google.it/intl/it/streetview/privacy/: fornisce le norme sulla privacy di Google Street View.

https://www.whatsapp.com/security/?l=it: fornisce le informazioni sulla sicurezza dell'applicazione Whatsapp.

https://trec.trentinosalute.net/web/guest: portale della piattaforma elettronica TreC della Provincia Autonoma di Trento.

https://investor.fb.com/home/default.aspx: sito web ufficiale della società Facebook che fornire tutti i dati sul bilancio, le statistiche e i termini di servizio.

https://myaccount.google.com/?hl=it: portale dell’account Google che consente di modificare il livello di protezione e controllo sui propri dati personali raccolti dai servizi.

https://www.google.it/intl/it/policies/privacy/: fornisce le norme sulla privacy di Google.

https://www.google.it/intl/it/policies/technologies/: fornisce i principi sulla privacy di Google.

http://www.ryerson.ca/pbdi/privacy-by-design/certification/: sito web ufficiale del meccanismo di certificazione del Privacy and Big Data Institute della Ryerson University.

The Student Paper Series of the Trento Lawtech Research Group is published since Fall 2010

http://www.lawtech.jus.unitn.it/index.php/student-paper-series?start=1

Freely downloadable papers already published:

STUDENT PAPER N. 34
La dimensione giuridica del Terroir

BERTINATO, MATTEO (2017), La dimensione giuridica del Terroir, Trento Law and Technology Research Group. Student Paper Series; 34. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-728-0

STUDENT PAPER N. 33
La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito

MARISELLI, DAVIDE (2017), La gravità del fatto nella commisurazione del danno non patrimoniale: un'indagine (anche) nella giurisprudenza di merito, Trento Law and Technology Research Group. Student Paper Series; 33. Trento: Università degli Studi di Trento. ISBN: 978-88-8443-727-3

STUDENT PAPER N. 32
«Edible insects». l'Entomofagia nel quadro delle nuove regole europee sui novel foods

TASINI FEDERICO (2016), «Edible insects». l'Entomofagia nel quadro delle nuove regole europee sui novel foods = «Edible Insects»: Entomophagy in light of the new European Legislation on novel Foods, Trento Law and Technology Research Group. Student Paper Series; 32. Trento: Università degli Studi di Trento. ISBN 978-88-8443-709-9

STUDENT PAPER N. 31
L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi

TAUFER FRANCESCO (2016), L'insegnamento dello sci: responsabilità civile e assicurazione per danni ad allievi o a terzi, Trento Law and Technology Research Group. Student Paper Series; 31. Trento: Università degli Studi di Trento. ISBN 978-88-8443-697-9

STUDENT PAPER N. 30
Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo

MAGGIOLO ANNA (2016), Incrocio tra Contratti e Proprietà Intellettuale nella Innovazione Scientifica e tecnologica: il Modello del Consortium Agreement europeo, Trento Law and Technology Research Group. Student Paper Series; 30. Trento: Università degli Studi di Trento. ISBN 978-88-8443-696-2

STUDENT PAPER N. 29
La neutralità della rete

BIASIN ELISABETTA (2016) La neutralità della rete, Trento Law and Technology Research Group. Student Paper Series; 29. Trento: Università degli Studi di Trento. ISBN 978-88-8443-693-1

STUDENT PAPER N. 28
Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law

ACERBI GIOVANNI (2016) Negotiation Bases and Application Perspectives of TTIP with Reference to Food Law. The Trento Law and Technology Research Group. Student Paper Series; 28. Trento: Università degli Studi di Trento. ISBN 978-88-8443-563-7

STUDENT PAPER N. 27
Privacy and Health Data: A Comparative analysis

FOGLIA CAROLINA (2016) Privacy and Health Data: A Comparative analysis. The Trento Law and Technology Research Group. Student Paper Series; 27. Trento: Università degli Studi di Trento. ISBN 978-88-8443-546-0

STUDENT PAPER N. 26
Big Data: Privacy and Intellectual Property in a Comparative Perspective

SARTORE FEDERICO (2016) Big Data: Privacy and Intellectual Property in a Comparative Perspective. The Trento Law and Technology Research Group. Student Paper Series; 26. Trento: Università degli Studi di Trento. ISBN 978-88-8443-534-7

STUDENT PAPER N. 25
Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course

REMO ANDREOLLI, DALILA MACCIONI, ALBERTO MANTOVANI, CHIARA MARCHETTO, MARIASOLE MASCHIO, GIULIA MASSIMO, ALICE MATTEOTTI, MICHELE MAZZETTI, PIERA MIGNEMI, CHIARA MILANESE, GIACOMO MINGARDO, ANNA LAURA MOGETTA, AMEDEO MONTI, SARA MORANDI, BENEDETTA MUNARI, EDOARDO NADALINI, SERENA NANNI, VANIA ODORIZZI, ANTONIA PALOMBELLA, EMANUELE PASTORINO, JULIA PAU, TOMMASO PEDRAZZANI, PATRIZIA PEDRETTI, VERA PERRICONE, BEATRICE PEVARELLO, LARA PIASERE, MARTA PILOTTO, MARCO POLI, ANNA POLITO, CARLO ALBERTO PULEJO, SILVIA RICCAMBONI, ROBERTA RICCHIUTI, LORENZO RICCO, ELEONORA RIGHI, FRANCESCA RIGO, CHIARA ROMANO, ANTONIO ROSSI, ELEONORA ROTOLA, ALESSANDRO RUFFINI, DENISE SACCO, GIULIA SAKEZI, CHIARA SALATI, MATTEO SANTOMAURO, SILVIA SARTORI, ANGELA SETTE, BIANCA STELZER, GIORGIA TRENTINI, SILVIA TROVATO, GIULIA URBANIS, MARIA CRISTINA URBANO, NICOL VECCARO, VERONICA VILLOTTI, GIULIA VISENTINI, LETIZIA ZAVATTI, ELENA ZUCCHI (2016) Leggere (nel)la giurisprudenza: 53 sentenze inedite in tema di responsabilità civile nelle analisi di 53 annotatori in formazione = Reading (in) the caselaw: 53 unpublished judgemnts dealing with civil liability law analyzed with annotations and comments by 53 students during their civil law course. The Trento Law and Technology Research Group. Student Paper Series; 25. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 24
La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile= The Digital Defective Product: 3D Product and Civil Liability

CAERAN, MIRCO (2016) La digitalizzazione del prodotto difettoso: stampa 3D e responsabilità civile = The Digital Defective Product: 3D Product and Civil Liability. The Trento Law and Technology Research Group. Student Paper Series; 24. Trento: Università degli Studi di Trento. ISBN 978-88-8443-663-4

STUDENT PAPER N. 23

La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities

CHIARUTTINI, MARIA OTTAVIA (2015) La gestione della proprietà intellettuale nelle università australiane = Intellectual Property Management in Australian Universities. The Trento Law and Technology Research Group. Student Paper Series; 23. Trento: Università degli Studi di Trento. ISBN 978-88-8443-626-9

STUDENT PAPER N. 22

Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio = Technology Transfer and Regional Context: Old Problems and New Perspectives for a Sustainable Co-operation among Universitiy, Entrepreneurship and Local Economy

CALGARO, GIOVANNI (2013) Trasferimento tecnologico e realtà locale: vecchie problematiche e nuove prospettive per una collaborazione tra università, industria e territorio. The Trento Law and Technology Research Group. Student Paper Series; 22. Trento: Università degli Studi di Trento. ISBN 978-88-8443-525-5

STUDENT PAPER N. 21

La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata = Internet Service Provider liability and copyright infringement: a comparative analysis.

IMPERADORI, ROSSELLA (2014) *La responsabilità dell'Internet Service Provider per violazione del diritto d'autore: un'analisi comparata.* Trento Law and Technology Research Group. Student Paper; 21. Trento: Università degli Studi di Trento. ISBN 978-88-8443-572-9

STUDENT PAPER N. 20

Open innovation e patent: un'analisi comparata = Open innovation and patent: a comparative analysis

PONTI, STEFANIA (2014) *Open innovation e patent: un'analisi comparata.* The Trento Law and Technology Research Group. Student Paper Series; 20. Trento: Università degli Studi di Trento. ISBN 978-88-8443-573-6

STUDENT PAPER N. 19
La responsabilità civile nell'attività sciistica

CAPPA, MARISA (2014) La responsabilità civile nell'attività sciistica = Ski accidents and civil liability. Trento Law and Technology Research Group. Student Paper Series, 19. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 18
Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM

TEBANO, GIANLUIGI (2014) Biodiversità agricola e tutela degli agricoltori dall'Hold-Up brevettuale: il caso degli OGM = Agricultural Biodiversity and the Protection of Farmers from patent Hold-Up: the case of GMOs.Trento Law and Technology Research Group. Student Paper Series; 18. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 17

Produrre e nutrirsi "bio": analisi comparata del diritto degli alimenti biologici

MAFFEI, STEPHANIE (2013) Produrre e nutrirsi "bio" : analisi comparata del diritto degli alimenti biologici = Producing and Eating "Bio": A Comparative Analisys of the Law of Organic Food. Trento Law and Technology Research Group. Student Paper Series; 17. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 16
La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata = The Protection of Geographical Indications in the Wine Sector: A Comparative Analisys

SIMONI, CHIARA (2013) La tutela delle indicazioni geografiche nel settore vitivinicolo: un'analisi comparata. The Trento Law and Technology Research Group. Student Papers Series; 16. Trento: Università degli Studi di Trento. Facoltà di Giurisprudenza.
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
142.

STUDENT PAPER N. 15
Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano

SALVADORI, IVAN (2013) Regole di sicurezza e responsabilità civile nelle attività di mountain biking e downhill montano. Trento Law and Technology Research Group. Student Paper; 15. Trento: Università degli Studi di Trento.

STUDENT PAPER N. 14
Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare

VIZZIELLO, VIVIANA (2013) Plagio, proprietà intellettuale e musica: un'analisi interdisciplinare. Trento Law and Technology Research Group. Student Paper; 14. Trento: Università degli Studi di Trento.

STUDENT PAPER N.13
The Intellectual Property and Open Source Approaches to Biological Material

CARVALHO, ALEXANDRA (2013) The Intellectual Property and Open Source Approaches to Biological Material. Trento Law and Technology Research Group. Student Paper Series; 13. Trento: Università degli Studi di Trento.

STUDENT PAPER N.12
Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930)

TRESTINI, SILVIA (2012) Per un'archeologia del diritto alimentare: 54 anni di repertori giurisprudenziali sulla sicurezza e qualità del cibo (1876-1930) = For an Archeology of Food Law: 54 Years of Case Law Collections Concerning the Safety and Quality of Food (1876-1930). The Trento Law and Technology Research Group. Student Papers Series, 12.
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
143.

STUDENT PAPER N.11
Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo

PICCIN, CHIARA (2012) Dalle Alpi ai Pirenei: analisi comparata della responsabilità civile per attività turistico-ricreative legate alla montagna nel diritto italiano e spagnolo = From the Alps to the Pyrenees: Comparative Analysis of Civil Liability for Mountain Sport Activities in Italian and Spanish Law. The Trento Law and Technology Research Group. Student Papers Series, 11

STUDENT PAPER N.10
Copynorms: Norme Sociali e Diritto d'Autore

PERRI, THOMAS (2012) Copynorms: Norme Sociali e Diritto d'Autore = Copynorms: Social Norms and Copyright. Trento Law and Technology Research Group. Students Paper Series, 10

STUDENT PAPER N. 9
L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco

ALESSANDRA ZUCCATO (2012), L'export vitivinicolo negli Stati Uniti: regole di settore e prassi contrattuali con particolare riferimento al caso del Prosecco = Exporting Wines to the United States: Rules and Contractual Practices with Specific Reference to the Case of ProseccoTrento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 9)

STUDENT PAPER N.8
Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis.

RUGGERO, BROGI (2011) Equo compenso e diritto d'autore: un'analisi comparata = Fair Compensation and Author's Rights: a Comparative Analysis. Trento: Università degli Studi di Trento (TrentoLawand Technology Research Group. Student Papers Series, 8)
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
144

STUDENT PAPER N.7
Evoluzione tecnologica e mutamento del concetto di plagio nella musica

TREVISA, ANDREA (2012) Evoluzione tecnologica e mutamento del concetto di plagio nella musica = Technological evolution and change of the notion of plagiarism in music Trento:

Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 7)

STUDENT PAPER N.6
Il trasferimento tecnologico università-imprese: profili giuridici ed economici

SIRAGNA, SARA (2011) Il trasferimento tecnologico università-imprese: profili giuridici ed economici = University-Enterprises Technological Transfer: Legal and Economic issues Trento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 6)

STUDENT PAPER N.5
Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese

GUERRINI, SUSANNA (2011) Conciliare la responsabilità medica: il modello "generalista" italiano a confronto col modello "specializzato" francese = Mediation & Medical Liability: The Italian "General Approach" Compared to the Specialized Model Applied in FranceTrento: Università degli Studi di Trento (Trento Law and Technology Research Group. Students Paper Series 5)

STUDENT PAPER N.4
"Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia

PODETTI, MASSIMILIANO (2011) "Gun Control" e Responsabilità Civile: una comparazione fra Stati Uniti e Italia = Gun Control and Tort Liability: A Comparison between the U.S. and Italy Trento: Università degli Studi di Trento. (Trento Law and Technology Research Group. Students Paper Series 4)
This paper is published in the Trento Law and Technology Research Group - Student Paper Series Electronic copy available at: http://eprints.biblio.unitn.it/archive/00004292/
145

STUDENT PAPER N.3
Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti

TOGNI, ENRICO (2011) Smart Foods e Integratori Alimentari: Profili di Regolamentazione e Responsabilità in una comparazione tra Europa e Stati Uniti = Smart Foods and Dietary Supplements: Regulatory and Civil Liability Issues in a Comparison between Europe and

United States Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 3)

STUDENT PAPER N.2
Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia

SARTOR, MARTA (2010) Il ruolo della responsabilità civile nella famiglia: una comparazione tra Italia e Francia = The Role of Tort Law within the Family: A Comparison between Italy and France Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students
Paper Series; 2)

STUDENT PAPER N.1
Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito

RIZZETTO, FEDERICO (2010) Tecnologie belliche e danno al proprio combattente: il ruolo della responsabilità civile in una comparazione fra il caso statunitense dell'Agent Orange e il caso italiano dell'uranio impoverito = War Technologies and Home Soldiers Injuries: The Role of Tort Law in a Comparison between the American "Agent Orange" and the Italian "Depleted Uranium" Litigations Trento: Università degli Studi di Trento - (Trento Law and Technology Research Group. Students Paper Series; 1)