Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO E NUOVE TECNOLOGIE
curriculum "Informatica Giuridica e Diritto dell'Informatica"

Ciclo XXIX

Settore Concorsuale di afferenza: 12-H3

Settore Scientifico disciplinare: IUS/20

NUOVI SCENARI DI RISCHIO E MISURE USER-CENTRIC PER LA PROTEZIONE DEI DATI PERSONALI

Presentata da: Dott.ssa Daniela Prestipino

Coordinatore Dottorato	**Relatore**
Prof. Giovanni Sartor	Prof.ssa Rebecca Montanari

Esame finale anno 2017

PREFAZIONE

Nello sviluppare il progetto di ricerca connesso al presente elaborato – *Nuovi scenari di rischio e misure user-centric per la protezione dei dati personali,* al susseguirsi delle varie questioni aperte riscontrate ho spesso avvertito la sensazione di chi tenta di svuotare l'oceano con un bicchiere: inquadrato un problema se ne aprivano di nuovi, differenti per prospettive, caratteristiche e sfide; una sensazione che si rafforzava ogni qual volta che i due sistemi regolatori: giuridico - che configura e indirizza la tutela la persona, e tecnico - che analizza, (ri)utilizza e protegge le informazioni personali, si interconnettevano per configurare la *privacy* e la protezione dei dati personali. Due sistemi ai quali, oggi, a conclusione del progetto, aggiungerei quello economico che eterodireziona le decisioni, e quello ed etico che punta a garantirne l'*accettabilità* e la *sostenibilità.*

Un'interconnessione che il nuovo Regolamento Europeo sulla protezione dei dati personali ha rafforzato e compiutamente riconosciuto, necessaria per un qualunque utilizzo corretto e *sostenibile* delle informazioni digitali, ed in particolare dei dati personali la cui protezione è stata definitivamente consacrata come un diritto fondamentale europeo della persona; ma altrettanto complessa per i limiti che tanto il diritto quanto la tecnologia continuamente presentano nell'affrontare fattivamente problemi tutti nuovi, immersi in un mondo tutto digitale che ciclicamente con velocità crescente e costi sempre minori interconnette e consuma informazioni, relaziona dati e *cose* per produrre conoscenza.

Un *exaflood* di informazioni che sta trasformando la persona *smaterializzandola*, al quale concorrono l'esplosione dei *social media*, soluzioni tecnologiche condivise come il *Cloud*, flessibili e pervasive come il *mobile* e l'*IoT* (*Internet of Things*), inferenziali e deduttive come i *Big Data* e il *Data Mining*. Un mondo talmente innervato di tecnologia da rendere anacronistico se non inutile il distinguo tra reale e digitale, e tale da imporre un radicale ripensamento sul limite perimetrale (sempreché ancora ipotizzabile e materiale) tra la sfera pubblica e quella privata, tra esterno ed interno, rispettivamente dal quale e sul quale, si è tradizionalmente tracciata la direzione dell'intromissione e dell'intrusività.

Un ambiente informazionale in cui si registra, si *scrive* e si memorizza tutto, ancor prima di valutare ciò che effettivamente serve ed è veramente importante; si *condivide* tanto senza conoscerne i rischi e valutarne le implicazioni, si cancella sempre meno; ma soprattutto in cui il ruolo di interprete e discriminante dell'importanza dell'informazione - quella da trattenere e considerare, è sempre più svolto da artefatti algoritmici *(find engine)* piuttosto che dalle persone.

Questa (sovra) abbondanza di dati che comunque *concerne* e *identifica* la persona, il soggetto interessato, essendone il principale alimentatore, se per un verso e nella misura in cui esprime relazioni semantiche significative, rappresenta un'opportunità straordinaria di miglioramento della società e delle

relazioni tra le persone (rivoluzionando entrambe), per un altro innesca implicazioni negative, sottili e non sempre distinguibili, connesse alla deduzione e alla messa in circolo di informazioni che possono essere preziose ma anche di scarsa qualità; di valore e vantaggiose per alcuni soggetti ma anche inutili e fuori contesto, o peggio rivelarsi dannose o destabilizzanti per la persona che le produce.

Si configura, quindi, un contesto informazionale distinto dall'utilizzo sempre più intensivo, sofisticato, irrinunciabile di dati personali su cui applicazioni e servizi ne basano funzionalità e successo; un contesto di cui la persona ne è sempre più parte, ma al contempo meno partecipe e più marginale rispetto alla compresenza di nuovi attori (oggetti informazionali; *Big Data Analytics* e *Data Miner*) che raccolgono e relazionano dati per trovare informazioni, per esporre i benefici della personalizzazione e migliorare la *on-line user-experience*; ma al contempo un contesto volto ad assumere decisioni, delineare profili spendibili sul mercato, pilotare scelte e decisioni degli individui, predigere e omologare comportamenti e attitudini; quindi ciclicamente influenzare ed eterodirigere il rilascio di nuove informazioni per, in definitiva, veicolare profitti basati su una totale libertà di *commercializzazione* e *compravendita* di informazioni personali.

In questo scenario il ruolo della *privacy* intesa come (diritto alla) protezione dei dati personali si riconfigura come insieme di azioni che oppongono, puntando a riequilibrarla, la crescente asimmetria tra l'*autodeterminazione individuale* (in cui convergono e trovano espressione le singolarità, le eccezionalità e le prerogative della persona) e il *determinismo informazionale* (in cui converge la superiorità elaborativa di *smart devices* sempre più numerosi, presenti, silenziosi e pervasivi, e di *Big Data Analytics* sempre più capaci di autoregolazione e autoapprendimento).

La protezione dei dati personali rappresenta, quindi, uno strumento di difesa non solo delle informazioni intese nella loro circolazione e dinamicità e degli enormi vantaggi che derivano dal loro utilizzo ma - per il tramite dell'autodeterminazione esercitabile su di esse, uno strumento di tutela della persona, dei suoi diritti, dei suoi valori e, quindi, della sua dignità. Uno strumento da cui dipende il successo e l'affermazione futura di modelli informazionali come i *Big Data* e *IoT*.

La protezione dei dati personali si affema come uno strumento volto a ristabilire una sorta di *ri-centralizzazione* dell'individuo affinché, in assenza di *privacy,* la *smaterializzazione* (inevitabile in contesti di socializzazione digitale) non degeneri in *snaturazione* e *deumanizzazione* - quindi in forme esclusione, quando alla persona viene pregiudicata e compromessa la prerogativa di valutare e compiere scelte consapevoli, libere e prive di condizionamenti algoritmici, indotte da fuorvianti convenienze.

Una *ri-centralizzazione* della persona che le misure regolatorie di carattere normativo ed espresse nel nuovo Regolamento Europeo per la protezione dei dati personali 679/2016, hanno consolidato e rafforzato nei principi ma non con altrettanta efficacia nella pratica.

LEGENDA E ABBREVIAZIONI

Anonimizzazione	Anonimato
APIs	Application Programming Interface
CA	Certification Authority
CODICE	Decreto Legislativo 30 Giugno 2003 n.196, codice in materia di protezione dei dati personali
CDR	Call Data Record
CRS	Conflict resolution Service
CVS	Credential Validation Services
Direttiva	Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, 24 ottobre 1995
GDPR	General Data Protection Regulation (UE) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016
GPS	Global Positioning System
H2020	Horizon 2020, The EU Framework Programme for Research and Innovation
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technologies
IdP	Identity Provider
IEEE (I3E)	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
MSPD	Multiple Subjects Personal Data
NFC	Near Field Communication
OASIS	Organization for the Advancement of Structured Information Standards
OD	Open Data
Opt-in, Opt-out	Option-in, Option-out
OS	Obligation Service
OTT	Over The Top
OWL	Ontology Web Language
P3P	Platform for Privacy Preferences
PA	Profile Authority
PAP	Policy Attribute Point
PAP	Policy Administration Point
PbD	Privacy by Design
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PDS	Personal Data Store
PETs	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
PII	Personal Identifiable Information

PIP	Policy Information Point
PKCS	Public-Key Cryptography Standards
PKI	Public key Infrastructure
RBAC	Rule-Based Access Control
RDF	Resource Description Framework
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SMIME	Secure/Multipurpose Internet Mail Extensions
SPARQL	Simple Protocol and RDF Query Language
TL/SSL	Trasport Layer Security/Secure Socket Layer
UDID	Unique Device Identifier
UE	Unione Europea
URI	Uniform Resource Identifier
VPI	Volunteered Personal Information
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WS-SECURITY	Web Services Security
WS-TRUST	Web Services Trust
X.509	X.509 Certificate
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

INDICE DELLE TABELLE E DELLE FIGURE

Figura i.1 – Evoluzione del concetto di *Privacy* e di protezione dei dati personali

Figura 2.1 – Andamento di crescita tra il 2015 e il 2010 del numero di devices e connessioni

Figura 2.2 – Comparazione e andamento di crescita del traffico *Cloud* nel periodo 2015-2020

Figura 2.3 – Data Never Sleeps 2.0 (anno 2014) e 4.0 (anno 2016)

Figura 2.4 – Utenti attivi sui Social Media (su base mensile e aggiornati al 2016)

Figura 2.5 – Distribuzione percentuale della quota di mercato della pubblicità on-line tra i principali Social Media

Figura 2.6 – Tipologie di dati personali e identificabilità della persona

Figura 2.7 – Il tipico ciclo di vita dell'informazione adattato al trattamento dei dati personali

Figura 2.8 – Ciclo di gestione dell'*advertising mirato*

Figura 2.9 – Mappa dei dati personali

Figura 2.10 – Modellazione della *Privacy*

Figura 2.11 – Report Verizon 2016: numero di incidenti di sicurezza nell'anno 2015 per settore coinvolto e dimensione di azienda

Figura 2.12 – Percezione di controllo sui dati personali

Figura 2.13 – Divulgazione dei dati personali

Figura 2.14 – Rischi e responsabilità relative alle informazioni personali fornite *online*

Figura 2.15 – Percezione del rischio connesso alla gestione di dati personali da terze parti

Figura 2.16 – Gestione delle politiche di P*rivacy*

Figura 3.1 – Trattamento di *anonimizzazione*

Figura 3.2 – Trattamento di pseudonimizzazione

Tabella 3.1 – Valutazione comparativa delle tecniche di anonimizzazione per randomizzazione

Tabella 3.2 –Valutazione comparativa delle tecniche di anonimizzazione per generalizzazione

Figura 3.3. - Esempio di *Sticky Privacy Policies*

Figura 3.4. - Componenti di un sistema *Policy Based Access Control (PBAC)*

Figura 3.5. - Proprietà di un sistema Policy Based Access Control (PBAC)

Figura 3.6. - Incrocio Proprietà/Framework di un sistema *Policy Based Access Control (PBAC)*

Figura 4.1 – Devices sensorizzati componenti l'*Internet of Things*

Figura 4.2 - Architettura *IoT* del progetto Energy@Home

Figura 4.3 - Confronto tra *web apps* e *apps* ibride

Figura 4.4 – Big Data e il paradigma delle 4 V: Volume, Velocità, Varietà e Veracità

Figura 4.5 – Paradigma 3V+3V dei *Big Data*

Figura 4.6 – Contesti *Smart Data* e *Big Data*

Figura 4.7 – *Data accretion* e re-identificazione.

Figura 4.8 – Nuovo scenario di vulnerabilità e di rischi per la protezione dei dati personali.

Tabella 4.1 - Le nuove forme di vulnerabilità e di rischio per la protezione dei dati personali.

Figura 4.9 – Le funzionalità e i servizi di un *Personal Data Store*.

Figura 4.10 – Area riservata del sito Trenitalia-Le frecce: aggiorna i tuoi dati per 10 Euro.

Figura 5.1. - Nuova Modellazione della *Privacy*.

INDICE

PREFAZIONE

LEGENDA E ABBREVIAZIONI

INDICE DELLE TABELLE E DELLE FIGURE

ABSTRACT

INTRODUZIONE

1. Il contesto di riferimento. p. 19
2. Le questioni aperte. Motivazione e obiettivi della ricerca. p. 26
3. I contributi della tesi. Approccio e metodologia. p. 29
4. La struttura della tesi. p. 33

CAPITOLO 1
LO SCENARIO NORMATIVO ATTUALE. QUESTIONI APERTE.

1. Introduzione. p. 36
2. Dalla Direttiva madre 95/46/CE al Regolamento Generale sulla protezione dei dati (UE) 2016/679. p. 40
3. Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: *le principali novità.* p. 49
4. Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: *il soggetto interessato e il dato personale.* p. 61
5. Questioni aperte. p. 69

CAPITOLO 2

***PRIVACY* E PROTEZIONE DEI DATI PERSONALI: PLURALITÀ SEMANTICHE E CRITICITÀ.**

1. I dati e le informazioni personali. p. 75

   1.1. La proprietà del dato personale, la gestione e gli attori coinvolti. p. 86

   1.2. La centralità dell'utente nel *disclosure* dei dati personali. p. 93

   1.3. Ripensare il concetto di dato personale. p. 96

   1.4. La modellazione dei Dati Personali. p. 99

2. La *Privacy* e la protezione dei dati personali. p. 101

   2.1. I molteplici significati della *Privacy*. p. 105

   2.2. La modellazione della *Privacy*. p. 109

   2.3. La protezione dei dati personali: le criticità e i rischi connessi alla gestione del dato. p. 110

   2.4. La protezione dei dati personali: la centralità dell'utente tra *status quo,* trasparenza e controllo. p. 116

CAPITOLO 3

***PRIVACY* E PROTEZIONE DEI DATI PERSONALI: LE CONTROMISURE.**

1. Tecnologie per la protezione dei dati e delle informazioni personali. p. 126
   1.1. *Public Key Infrastructure*: brevi cenni. p. 126

2. Privacy-Enhancing Technologies. p. 128
   2.1. L'anonimato e la protezione dei dati personali. p. 129
      2.1.1. L'analisi tecnico-giuridica del trattamento di *anonimizzazione*. p. 134
      2.1.2. Le tecniche di *anonimizzazione*. p. 140
      2.1.3. La *pseudonimizzazione*. p. 144
      2.1.4. Il diritto all'anonimato: profilo e identificabilità della persona. p. 146

3. I sistemi di *Privacy Policies-Preferences*. p. 149
   3.1. Le *Privacy Policies* di tipo "*provider centered*". Esempi. p. 150
   3.2. Le *Privacy Policies* di tipo *"User-centric" e "Data-centric". Sticky Privacy Policies.* p. 155
   3.3. I *Framework* e i linguaggi. p. 159

4. Questioni aperte. p. 162

5. La protezione dei dati personali come requisito intrinseco di processi e servizi. p. 164
   5.1. Il *framework Privacy by Design e Privacy by Default.* p. 164

CAPITOLO 4

VERSO LA *PRIVACY 2.0:* NUOVI SCENARI DI RISCHIO E NUOVE SEMANTICHE.

1. Gli scenari ed alcuni esempi di rischio in contesti di forte inferenza informativa. p. 167

   1.1. "*Internet of Things*". p. 171

   1.2. *App* per *smart-devices.* p. 177

   1.3. "*Big Data*" e *Data Mining*. p. 182

   1.4. Realtà aumentata e *Data Accretion* p. 188

2. Le nuove forme di vulnerabilità e di rischio per la protezione dei dati personali. p. 192

   2.1. Asimmetria Informativa. Dispersione del controllo sui dati personali. Perdita di qualità del consenso. p. 197

   2.2. Difetto di trasparenza. Eccesso di dati personali. Molteplicità delle finalità. p. 200

   2.3. Eccesso di esposizione dell'utente. Deduzione invasiva di profili. p. 202

   2.4. Difetto di *Privacy by Design/Default*. Pluralità dei titolari di trattamento. p. 203

3. La garanzia di qualità dei dati e le nuove tipologie di rischio per la *Privacy*. p. 205

4. Le nuove proprietà del Dato Personale. p. 209

   4.1. Proprietà e possesso del Dato Personale. *Personal Data Store.* p. 209

   4.2. I dati personali a soggetti multipli. *Multiple Subjects Personal Data.* p. 213

   4.3. Il valore economico dei Dati Personali e della *Privacy*. p. 215

CAPITOLO 5

PROGETTAZIONE DI UN MODELLO DI SUPPORTO A POLITICHE DI *PRIVACY* DI TIPO *USER* E *DATA CENTRIC.*

1. L'applicazione delle *Privacy Policies* di tipo *User-centric*. p. 220

   1.1. L'utilizzo delle *Sticky Privacy Policies* per la protezione di un *Multiple Subject Personal Data Store*. p. 224

   1.2. L'implementazione di una *Sticky Privacy Policy* per la gestione della lista contatti dell'*App* di messaggistica *WhatsApp Messenger*. p. 230

2. Nuove Ontologie di Dati Personali e di *Privacy*. p. 233

CONCLUSIONI p. 238

APPENDICE
DICHIARAZIONE DEI DIRITTI IN INTERNET (2015)

BIBLIOGRAFIA

1. Testi. p. 258
2. Provvedimenti e normativa Italiana e Comunitaria. p. 259
3. Banche dati e risorse elettroniche. p. 262

ABSTRACT

Il ricorso alle tecnologie *data intensive* e al trattamento digitalizzato delle informazioni, divenuto struttura portante di ogni relazione sociale, se per un verso persegue opportunità di benessere e sviluppo, vantaggi economici e progressi migliorativi della qualità di vita delle persone per un altro - quello attinente le modalità di presidio e di tutela delle informazioni personali, ha esacerbato problemi vecchi configurandone di nuovi.

Questi ultimi trovano collocazione in una drastica ricalibratura della sfera privata divenuta più dilatata, sovrapposta e confusa con quella pubblica, in risposta non solo alle sollecitazioni tecnologiche ma soprattutto all'affermarsi del soggetto interessato quale principale e centrale produttore di dati personali. L'abbattimento perimetrale tra i due ambiti rende limitativo se non fuorviante continuare a ritenere la violazione dei dati personali riconducibile (prevalentemente) ad intromissioni volontarie aventi una direzione di intrusività procedente dall'esterno verso l'interno e poste in essere da attori estranei o terzi.

Ciò indirizza che la riformulazione del concetto di *privacy* e protezione dei dati personali in contesti *data intensive* e *disruptive technologies* - e quindi delle relative contromisure, possa passare per una parallela, necessaria e non semplice ridefinizione delle tipologie di vulnerabilità e di rischio rispetto alle violazioni di sicurezza tradizionalmente volte contro la confidenzialità, l'integrità e la disponibilità delle informazioni, le quali tra l'altro non sempre hanno trovato nelle misure regolatorie o tecnologiche reazioni sistemiche, adeguate, tempestive, efficaci e commercialmente convincenti.

Rispetto a queste questioni aperte, il contributo del progetto di ricerca si è mosso nella convinzione – peraltro novità portante del nuovo Regolamento Europeo 679/2016 sulla protezione dei dati personali, che rischi e vulnerabilità di *privacy* non possono più essere misurati (solo) *ex post* a violazione avvenuta e a danno fatto.

Essi devono essere (soprattutto) valutati *ex ante;* trovare iniziale previsione *by default/design* nella progettazione e nell'avvio stesso del trattamento; nonché essere inseriti in una configurazione che mantenga un collegamento tanto con la responsabilità del titolare e del responsabile - che il novellato regolatorio declina in termini di una vera e propria *assunzione di rischio,* tanto con l'affermarsi dell'utente come figura centrale che volontariamente *produce, rilascia e condivide* informazioni personali, tanto e non ultimo, con le proprietà contestuali - quantitative e qualitative, di tali informazioni comprese quella di essere condivise e relazionate tra una molteplicità di soggetti e, oggi, sempre più tra *cose interconnesse* e *artefatti algoritmici.*

Ciò premesso il contributo della ricerca si è sviluppato su tre dimensioni:

i. la prima di carattere concettuale mette a sistema, sulla base delle più importanti posizioni rintracciate in letteratura, i nuovi elementi caratterizzanti la protezione dei dati personali sulla base di: *a)* una profonda rimodulazione della centralità dell'utente rilevabile sia in fase di *disclosure* delle informazioni personali, sia in fase di impostazione delle *preferences* di *privacy; b)* una caratterizzazione del dato personale tanto per la sua funzione identificativa del soggetto interessato, tanto per i requisiti di qualità, nonché per la necessità di un suo ripensamento descrittivo e di formato; *c)* di un'analisi sull'evoluzione stessa del concetto di *privacy* e di protezione dei dati personali;

ii. la seconda di carattere analitico: *a)* illustra le limitazioni delle azioni regolatorie - sia tecniche che normative, nella misura in cui le prime – distinte in misure di sicurezza, in misure basate su politiche d'uso e in *Privacy Enhancing Technologies* – mancano di un sistema implementativo unitario e comprensivo; e le seconde mantengono un approccio alla protezione dei dati personali di tipo *top-down,* in cui il rafforzamento del principio dell'*accontability* del titolare e del responsabile non risulta essere stato contro-bilanciato da un parallelo *empowerment* del soggetto interessato; *b)* introduce nuove vulnerabilità di *privacy* in contesti distinti da una pluralità titolari e di soggetti interessati e da una forte inferenza informativa (quantitativa e qualitativa); queste possono essere misurabili *ex ante* in termini di un degrado di qualità dei dati e comprendono: l'asimmetria informativa tra chi produce le informazioni e chi le sfrutta; la massimizzazione quantitativa dei dati utilizzati; il degrado della qualità del consenso; il proliferare delle incontrollate finalità di utilizzo; la perdita di controllo sulle informazioni personali, la perdita di trasparenza, l'eccesso di esposizione del soggetto interessato.

iii. la terza, di carattere maggiormente applicativo, suggerisce una semplice *Proof of Concept* a supporto della validità delle argomentazioni di cui al precedente punto *ii.b.:* utilizza come contesto applicativo l'App *WhatsApp Messenger,* modella la rubrica contatti di un utente *WhatsApp* come un *Personal Data Store* a soggetti multipli *(Multiple Subjects Personal Data Store),* propone un modello implementativo di supporto in cui vengono intersecate le regole d'uso di ogni utente. Nello specifico viene dimostrato: *a)* la carenza di trasparenza e informativa in ragione di ambiguità e lacune rintracciate nel *Privacy Notice* regolatorio esposto da *WhatsApp; b)* la conseguente ricorrenza di alcune nuove vulnerabilità per i dati personali rilasciati e condivise tramite l'App (asimmetria

informativa, eccesso di dati utilizzati, perdita di controllo) opponibili mediante regole d'uso *user-centric* di tipo *Sticky Privacy Policies*. Questa scelta sfrutta la prerogativa delle *Sticky Privacy Policies* – quale contenitore di regole definite dall'utente ed integrato ai dati da controllare, di poter essere agganciate alla lista contatti di un utente, consentendo a questi di filtrare – in fase di *disclosure,* il rilascio di informazioni personali gestite dall'App mantenendone il controllo durante il successivo utilizzo.

In chiusura viene proposto un set di nuovi descrittori semantici associabili ad altrettante proprietà del dato personale, affinché la modellazione ricavabile supporti, in prospettiva, una ottimale definizione e esecuzione di politiche di *privacy* di tipo *user e data centric*.

INTRODUZIONE

SOMMARIO: 1. Il contesto di riferimento. – **2.** Le questioni aperte. Motivazione e obiettivi della ricerca. – **3.** I contributi della tesi. Approccio e metodologia. – **4.** La struttura della tesi.

1. IL CONTESTO DI RIFERIMENTO.

Alla prima lettura del titolo dei due fondamentali atti regolamentari comunitari in materia di protezione dei dati personali - il Regolamento 2016/679[1] (GDPR) e la Direttiva 95/46/CE[2] (Direttiva), seguì nell'immediato da una riflessione connessa alla declinazione che accompagna entrambi e che nelle due versioni (inglese e italiano), recita:

> ….*on the protection of* ***individuals*** *(natural persons[3]) with regard to the processing of* ***personal data*** *and on the* ***free movement*** *of such data*;
>
> ….*relativa (relativo) alla tutela (protezione[4]) delle* ***persone fisiche*** *con riguardo al trattamento dei* ***dati personali****, nonché alla* ***libera circolazione*** *di tali dati*;

Tale riflessione – associata a quella che appariva come una palmare contraddizione in quel frangente compensata dalla spartanità descrittiva del Decreto Legislativo Italiano 196/2003[5]: *codice in materia di protezione dei dati personali* (CODICE) - riguardava la compresenza di due concetti se non opposti, comunque non immediatamente sovrapponibili:

1) la ***protezione*** dei dati personali - strumentale alla protezione delle persone intese nella loro fisicità;
2) e la ***libera*** circolazione degli stessi dati - intesi (in quanto digitali) nella loro nativa immaterialità.

Nel corso dello svolgimento del programma di ricerca è emerso come poche righe potessero contenere gli elementi cardini connessi alla *gestione* delle informazioni personali - quindi alla *privacy* e alla protezione dei dati personali, se considerate *entità* e *beni* di un mondo

---

1 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - L 119/34, pubblicato nella GUUE del 4.5.2016*.

2 Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995*, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, L 281/31, pubblicato nella GUUE del 23.11.1995*.

3 (*Of natural persons*) termine presente nel Regolamento 2016/679.

4 *Protezione*, termine presente nella traduzione italiana del Regolamento Europeo 2016/679.

5 Il Decreto Legislativo 30 Giugno 2003 n.196, *codice in materia di protezione dei dati personali, pubblicato nella GURI n. 174 del 29 luglio 2003*.

sempre più digitale, dinamico, imprevedibilmente collaborativo, *tipizzato* e accessibile[6] tale da ispirarne la disamina secondo i principi dell'*abbondanza* piuttosto che della *scarsità*[7]; valutare la *protezione* dei dati personali come questione contestuale piuttosto che specifica; estesa piuttosto che individuale; quindi i diritti, le responsabilità, le risultanti *capabilities,* i permessi di accesso, di utilizzo e di divulgazione come un fatto condiviso (dinamico) piuttosto che esclusivo (statico).

Tutto ciò ha preliminarmente richiesto un necessario inquadramento del contesto di riferimento iniziale, sommatoria di quattro elementi principali e del loro ricalibrarsi in relazione all'inarrestabile affermarsi delle nuove e *dirompenti* tecnologie: *a)* il soggetto interessato (la persona, l'utente); *b)* il dato personale (la sfera privata); *c)* il significato di *privacy* e di protezione delle informazioni personali; *d)* le misure regolatorie: normative e tecniche.

L'ambiente digitale attuale in cui viviamo evolve a velocità crescenti verso uno scenario c.d. *DataGeddon*[8]: *data intensive*, pervasivo, interconnesso, innervato e aumentato di tecnologia, distinto da un continua e voluminosa raccolta di informazioni, sempre più veloce e meno costosa nello scambio e nell'archiviazione. Il potenziale di inter-relazione semantica e di inferenza che ne deriva è comunemente indicato come *schema Big Data.* Questo fenomeno ha per artefici le *Internet disruptive technologies*[9] - in particolare quelle mobili (*Tablet*, *Smartphone*, *Laptop*), e gli *smart objects* (*Internet of Things*), e per oggetto il mondo e la persona; su quest'ultima incide sotto due punti di vista parimenti significativi anche se con differenti gradi di evidenza.

Se da un lato la crescente digitalizzazione di artefatti, servizi e di ogni attività sociale ha creato indubbie opportunità di benessere e sviluppo, vantaggi economici e progressi scientifici, migliorando la qualità di vita degli individui, per un altro lato questa trasformazione è stata talmente veloce, intensa e profonda da innescare un progressivo assorbimento dell'ambiente reale in quello digitale, con l'implicazione (tra le altre) di migrare e *dislocare* la persona in un

---

6 Non secondariamente anche sotto il profilo dei costi, della disponibilità di banda e della connettività.

7 Gli economisti parlano di "*economia della scarsità*" e di "*economia dell'abbondanza*", descrivendo i due metodi con cui chi controlla i mezzi di produzione di un certo bene in un dato mercato cerca di massimizzare il proprio profitto alzando i prezzi di un bene, con conseguente mercato di dimensioni ristrette e alti margini di profitto, in tale situazione; oppure abbassando i prezzi ed ampliando al massimo le dimensioni del mercato, con conseguenti bassi margini di profitto ma grandi volumi economici.
In argomento cfr: MARCO CALAMARI, *Economia dell'abbondanza o della scarsità*, Punto Informatico, 05 Settembre 2003. http://punto-informatico.it/350871_2/PI/Commenti/economia-della-scarsita-dell-abbondanza.aspx

8 Con il termine *DataGeddon*, viene indicato il crescente volume di dati che vengono raccolti, gestiti e custoditi. In argomento
cfr: http://www.datacenterknowledge.com/archives/2015/11/02/datageddon-data-center-location/

9 Con il termine Internet *disruptive technologies* si intende raggruppare l'insieme delle tecnologie (interconnesse in rete) di rivoluzionario e al limite destabilizzante impatto innovativo: *Internet of Things, Cloud Computing, Mobile, Robotics,* distinte dallo scambio continuo e massivo di grandi volumi di dati. In argomento
cfr http://www.intelligenthq.com/technology/12-disruptive-technologies/

mondo fatto in larga misura da informazioni, in un certo senso *spersonalizzandola* tendendo a farne gradualmente affermare (e prevalere) una sorta di *materialità* e *produttività informazionale,* che la trasforma da individuo singolare e consapevole a profilo fortemente tipizzato, in misura sempre maggiore smaterializzato e modellato da una sorta di determinismo informazionale prerogativa di chi tratta, gestisce e processa le informazioni. Tutto ciò rischia di estorcere il senso e il significato di identità personale, con intuibili e significative implicazioni sulla costruzione della propria personalità, sulla capacità di partecipazione, di scelta e di autodeterminazione nonché di mantenimento nel tempo del governo sulle proprie informazioni e sul loro processamento.

Con riferimento a questa trasformazione in atto, meno sensazionale rispetto ai palmari benefici apportati dalle *ICT* (*Information and Communiction Technologies*) ma non meno rilevante e significativa, si ritiene significativo accennare a due posizioni italiane contemporanee che pur con stili e per finalità diverse convergono nel motivarla e sostenerla: quella del filosofo Luciano Floridi[10] (che osserva la questione dal punto di vista metafisico ed etico) e del costituzionalista Stefano Rodotà[11] (che ne rileva il necessario evolvere dei diritti fondamentali da tradizionali a diritti della Rete).

Luciano Floridi – *La quarta rivoluzione*, ritiene le Internet *ICT* stiano attuando una vera e propria *quarta rivoluzione* (dopo quelle riconducibili a N. Copernico, C. Darwin e S. Fraud) poiché nel mutare radicalmente il mondo reale da materiale a digitale non si limitano a configurarlo e strutturarlo in un modo nuovo (migliorato e aumentato) ma ne ridefiniscono intrinsecamente la natura e il significato, la comprensione che la persona ha di esso, quindi di se stessa e del senso di identità personale. Un senso di identità personale eroso dall'essere *onlife* - ovvero dal progressivo trascorrere della vita *on-line* (tra gli *smart objects)*, dal divenire prodotto di massa *tipizzato* e dal conseguente abbattimento della singolarità individuale.

Senza voler eccedere in una prospettiva futura per quanto assai prossima, la conoscenza e l'identità sociale della persona passa sempre più dalla mole di informazioni digitali ad essa riferibili e trattate dalla tecnologia: "*Noi siamo i nostri dati*"- cfr Stefano Rodotà in *Il Mondo nella Rete. Quali i diritti, quali i vincoli*, in cui l'autore ne rileva l'accezione più preoccupante della questione[12].

---

[10] LUCIANO FLORIDI, *La quarta rivoluzione*, Codice Edizione 2012, cap. 1 pag. 10-22.

[11] STEFANO RODOTÀ, *Il mondo nella rete. Quali i diritti quali i vincoli.* Editori Laterza, 2014 cap. 4 -5 pag. 27 – 40.

[12] Sulla questione e l'interpretazione di S. Rodotà si indicano i seguenti ulteriori contributi:
Nel web 2.0 l'identità si fa comunicazione. Diventa disponibile per il data mining, per la considerazione della persona come una miniera a cielo aperto dalla quale estrarre continuamente qualsiasi dato. <...> Il mondo degli oggetti prende la parola, diventa fonte di dati che si traducono in un flusso crescente di informazioni sulle persone che hanno rapporti con tali oggetti. Gli oggetti dialogano tra di loro per accrescere

La persona tende ad essere sovrapposta e sostituita da un corrispondente *oggetto informazionale* produttore di dati personali, sul quale lavorano meccanismi di *find engine*[13]*,* algoritmi di *Data Mining,* funzioni di inferenza pensate e scritte per estrarre caratteristiche che a loro volta analizzate, sincronizzate, incrociate e aggregate producono, nel tempo, grandi volumi di dati, acquisiscono nuove informazioni relative ai comportamenti *identificanti* le persone singole o raggruppate sulla base di comuni caratteristiche; queste informazioni sono riutilizzate per finalità predittive, per *attribuire* abitudini, preferenze, frequentazioni; configurare profili.

L'aspetto singolare di questo processo è che il principale costruttore di questo *oggetto informazionale* è il soggetto stesso (la persona) che interviene (più o meno consapevolmente) sotto una duplice spinta:

i. quella di opporre il divenire un "*artefatto prodotto di massa*" esponendo (quasi esibendo) le proprie informazioni personali per essere meno anonimo e distinguersi da un punto di vista informazionale[14]; e secondariamente

ii. quella indotta dall'immediatezza e dalla capillarità tecnologica che ha affermato un rivoluzionato modo di pensare e di comunicare all'interno del quale la capacità di differire la risposta in una *chat* o in un post per valutare, ponderare il proprio riscontro, pensare alle implicazioni o alle parole *giuste da usare* è diventata sempre più difficile e inconsueta; parimenti trattenersi dalla tentazione di rispondere ad una chiamata, una mail, un *whatsapp* o di conoscere chi sta tentando di comunicare, quando, come e con quali frequenze; così come optare per il silenzio, oppure per il saper attendere e *stare da soli.*

Tutto ciò produce volumi di dati personali in larga misura pubblici per definizione (per *default settings*) e in quantità superiori a quelli effettivamente necessari.

---

e aggiornare continuamente i dati riguardanti le persone e trasferirli ad apparati che, a loro volta, li elaborano e ne traggono conclusioni riguardanti la persona interessata. <...> Diventa sempre meno proponibile una definizione dell'identità come "io sono quello che dico di essere", sostituita da un "tu sei quello che Google dice che sei".
cfr STEFANO RODOTÀ, *Il Diritto di avere diritti,* Laterza 2013

[13] Nella parte dell'elaborato che segue, l'espressione *find engine* indicherà l'insieme di applicazioni collocate generalmente in *cloud* che in risposta a specifiche richieste degli utenti, aggregano processano grandi volumi di dati per analizzarne gli attributi descrittivi (qualitativi e quantitativi) mediante algoritmi di definizione ed estrazione di attributi (tra gli altri: *data mining, machine learning, hashing, crowdsourcing*), al fine di estrarre collegamenti, effettuare analisi predittive, relazionare specifici fenomeni. Un tipica applicazione di *find engine* è il motore di ricerca.

[14] Gli indicatori di questa forma di riappropriazione e riaffermazione della propria personalità sono evidenti nella partecipazione attiva alle communities virtuali dei social media, dei blog e dei canali sociali, curando con costanza il proprio profilo; nell'affidare alle reti sociali immagini, opinioni, reazioni attinenti a fatti personali, altrui o a questioni connesse alla cronaca, alla politica e alla società in genere con un like, un tweet, un simbolo, una reazione; nel partecipare pubblicamente il proprio pensiero, lo stato d'animo o il proprio punto di vista.

Il configurarsi del soggetto interessato come principale *produttore* e *condivisore* di dati personali ha implicato una radicale trasformazione della sfera privata, la quale – anch'essa in risposta alla sollecitazione delle nuove tecnologie, è divenuta un contenitore di informazioni personali privo di perimetro, pressoché infinito e quindi indistinto dalla c.d. sfera pubblica; un dominio di informazioni, partecipato e condiviso:

i. *prodotte, rilasciate* e *cedute* (sempre più esibite) dagli stessi soggetti ogni qual volta utilizzano beni e servizi[15];
ii. *accedute* (in maniera sempre più semplice) da una molteplicità di attori: utenti, aziende, artefatti algoritmici, dispositivi e cose interconnesse;
iii. oggetto di accresciute e rinnovate le modalità di violazione, che la fusione della sfera pubblica con quella privata rende non più (solo) tracciabili su una direzione di intrusività e di dolosità procedente dall'esterno verso l'interno[16,17,18,19].

Quanto precede non poteva non implicare una speculare e altrettanto significativa trasformazione nelle modalità di presidio dei dati personali. I requisiti della *privacy* e della protezione dei dati personali riflettono il differenziarsi della nozione di *sfera privata,* dilatatasi sotto la spinta delle nuove tecnologie e in risposta ad un mutato ruolo del soggetto interessato; tecnologie che hanno fin dall'inizio hanno orientato le originarie coordinate legali della *privacy,* configurandola come diritto ad *essere lasciati (da) soli (the right to be let alone)*[20]. Tale definizione fu formulata nel 1890 da due giovani avvocati di Boston Samuel Warren e Louis Brandeis in risposta all'uso intrusivo della fotografia istantanea che – all'epoca veicolata dal diffondersi dei quotidiani di costume, rendeva pubblici aspetti della vita ritenuti privati. Questa concettualizzazione della *privacy* intesa come riservatezza e presidio della propria vita/sfera privata - nel senso letterale di *proprietà privata materiale* escludente ogni interazione con gli altri,

---

15 Le informazioni personali tendono ad essere meno private e sempre più oggetto di libera circolazione, trasferite in contro-valore quando il *disclosure* è indotto da vantaggi e compensazioni materiali di immediata convenienza; e - non secondariamente, sempre più esposte in pubblico dallo stesso utente perché segni visibili della propria personalità e delle quali l'utente si avvale per contrastare la tipizzazione, riaffermare e distinguere se stesso nel mondo digitale.

16 Le violazioni possono tradizionalmente differenziarsi dal furto (massivo) di credenziali di accesso; a tutte le svariate intromissioni finalizzate alla conoscenza, alla modifica e al controllo dell'identità della persona; al tracciamento delle sue attività e alla profilazione; alla perdita di dati, la modifica o l'utilizzo non autorizzato.
Cfr GDPR art. 4 *Definizioni,* comma 12) *«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.*

17 In argomento cfr: https://it.businessinsider.com/yahoo-si-e-fatta-anche-fregare-i-tuoi-dati-ecco-che-cosa-rischi-e-cosa-devi-fare/?ref=HREC1-22, *Yahoo! si è fatta anche fregare i tuoi dati: ecco che cosa rischi e cosa devi fare*, 18 Dicembre 2016

18 In argomento cfr: http://www.pagina99.it/2017/01/11/pubblicita-online-web-advertising-no-tutela-privacy-su-internet-informativa, *Pubblicità online, stiamo entrando nell'era della no-privacy su Internet* – 11 Gennaio 2017

19 Direttiva 2009/136/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009; Provvedimento del Garante per la protezione dei dati personali dell'8 maggio 2014, "*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*".

20 Cfr WARREN S., BRANDEIS L., *The Right to Privacy*, in Harvard Law Review, 1890, 4, p. 193-220

si mantiene sostanzialmente inalterata sino alla diffusione dei sistemi di trattamento digitale delle informazioni veicolate da reti pubbliche aperte, quando dal paradigma *statico* della riservatezza [persona, informazione, segretezza] si passa a quello *dinamico* della protezione e del controllo [persona, informazione, *circolazione,* segretezza][21].

Gli strumenti per attuare la protezione delle informazioni personali e quindi implementativi del loro controllo comprendono sia azioni regolatorie giuridiche sia misure specificatamente tecniche. Entrambe perseguono l'obiettivo di integrare nel trattamento e nella gestione dei dati personali le necessarie garanzie per tutelare i diritti e le libertà delle persone.

La Direttiva europea 96/46/CE e il Codice attuativo italiano (decreto legislativo 196/2003) rispettivamente introducono e affermano il diritto (fondamentale) alla protezione dei dati personali come diritto di controllo su qualsiasi informazione riguardante una persona che ne consenta l'identificazione diretta o indiretta. Questo controllo si attua per il tramite di una prerogativa decisionale e di autodeterminazione esercitata dai soggetti interessati, che subordina il (legittimo) trattamento delle informazioni personali: *i)* alla dichiarata, libera, specifica, informata volontà del soggetto interessato di volerlo accettare e acconsentire; nonché *ii)* alla necessaria rimodulazione di tale volontà per il tramite di tutta una serie di diritti di controllo azionabili dal soggetto interessato ogni qual volta il subentro di ulteriori e nuove finalità o secondari utilizzi dei dati personali, diversi da quelli connessi all'iniziale rilascio e raccolta, ne richiedono un ripensamento. Il nuovo Regolamento Europeo 679/2016 eredita e consolida questo principio di controllo rafforzando tanto il consenso - allorquando alle già esistenti condizioni aggiunge quella di essere *inequivocabile* e *concludente;* tanto i diritti di controllo azionabili dall'interessato perfezionando quelli esistenti e introducendone di nuovi quali il diritto alla cancellazione (oblio) e il diritto alla portabilità.

Le azioni tecniche a presidio e controllo delle informazioni personali comprendono misure volte sia alla riservatezza, sia al controllo d'uso dei dati personali, sia alla protezione dell'associazione identificativa [persona, informazione]. I diversi approcci distinguono misure di sicurezza finalizzate a garantire i requisiti di confidenzialità, di integrità e di disponibilità delle informazioni; sistemi di politiche e di regole il cui scopo è filtrare e controllare il rilascio, l'accesso e l'uso dei dati personali; e misure di *privacy* vere e proprie comprendenti le c.d. *Privacy Enhancing Technologies (PETs),* volte a minimizzare l'utilizzo di dati personali per perseguire una determinata finalità al punto - in condizioni di anonimizzazione, da non

[21] RODOTÀ S., *Privacy e costruzione della sfera privata*, in Id., "Tecnologie e diritti", Bologna, Il Mulino, 1995.

ritenersi più necessario un trattamento di dati personali.

La questione – principale punto aperto e filo conduttore di questo lavoro, è il mantenimento nel tempo di un efficace controllo sulla divulgazione e l'utilizzo dei propri dati personali in ragione dei diritti azionabili dall'interessato e delle misure tecniche utilizzabili. Un controllo che non può non essere condiviso tra le possibili parti coinvolte: soggetti interessati, titolari al trattamento, destinatari, terze parti e *stakeholders;* utenti, non-utenti, oggetti; così come non prescindere da fattori contestuali attinenti le caratteristiche dei dati, i diversi ambiti informazionali e nuovi scenari di vulnerabilità ad essi connessi.

In definitiva un controllo che rende fattibile e garantisce nel tempo l'armonizzazione del paradigma regolatorio portante: [*informativa* – *finalità* – *consenso*] con le nuove tipologie di trattamento *data intensive* distinte da una pluralità pressoché illimitata di finalità, da nuove e plurime tipologie di attori e il cui successo si fonda sull'imprescindibile utilizzo di dati personali ma al contempo sul prevenire – evitandone l'attuazione, il passaggio che trasforma l'*utente* – soggetto informato e inizialmente partecipe al ciclo di vita delle informazioni nella misura in cui lo alimenta, a *non utente* – attore non informato e inconsapevole delle implicazioni portate da nuove informazioni, lavorate da algoritmi diversi e per differenti scopi.

2. LE QUESTIONI APERTE. MOTIVAZIONE E OBIETTIVI DELLA RICERCA.

Le questioni aperte, connesse al contesto di riferimento illustrato nel precedente paragrafo, attengono: *i)* la ricalibrata centralità del soggetto interessato che si qualifica quale principale produttore di informazioni personali/identificative/private che diventano pubbliche per impostazione predefinita *(default settings)* e, come tali, origine di violazioni non previste; *ii)* la contestuale criticità per l'utente di controllarne il ri-utilizzo durante il ciclo di vita del trattamento che, sempre più allocato in contesti informazionali *data intensive,* processa e relaziona volumi di dati personali per finalità e utilizzi secondari differenti rispetto a quelli associati all'iniziale rilascio.

Questo macro-ambito di criticità può essere spacchettato in tre elementi rappresentativi di altrettante questioni aperte, relative:

1. al mancato bilanciamento della positivizzazione dell'*accountability* del titolare/responsabile del trattamento[22] con un pari *empowerment* del soggetto interessato: le regole di trattamento rimangono statiche, *top-down;* e il ruolo del soggetto - principale produttore di dati personali e il sostanziale destinatario della tutela, non centrale in molte questioni, prime fra tutte quella della valutazione e della successiva notifica delle violazioni ai dati personali;
2. alla limitazione dell'impianto regolatorio (normativo e tecnico) che - per quanto oltremodo consolidato nel ritenere e gestire la protezione delle informazioni personali come controllo sulle stesse, si è rivelato sostanzialmente non efficace nell'opporre violazioni sui dati personali intese come intromissioni volontarie e dolose volte alla distruzione, alla modifica, al furto o all'utilizzo illecito degli stessi e in misura sempre maggiore originate da informazioni personali o private rilasciate volontariamente dagli stessi soggetti, riutilizzate per scopi secondari e non previsti;
3. al permanere di tutte le azioni tecniche di protezione dei dati personali, siano esse basate su *PETs,* oppure sulla gestione delle politiche di accesso d'uso dei dati, o ancora su misure di sicurezza vere e proprie, speculari o staccate al trattamento (*add-on*) piuttosto che essere incorporate e native allo stesso (*embedded*); ciò implica l'assenza di

[22] Il nuovo Regolamento Europeo 679/2016 pur rafforzando le condizioni del consenso ed ampliando i diritti di controllo azionabili dall'interessato sul trattamento dei dati personali centra e pone sul titolare/responsabile e sull'Autorità di Controllo tutta la responsabilità del trattamento declinandola non più come un adempimento formale ma come una vera e propria *assunzione di rischio* e di *conformità* ai principi di protezione dei dati personali.
cfr GDPR art 24 *Responsabilità del titolare del trattamento* – art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* – art 28 - *Responsabile del trattamento*

automatismi nativi per la configurazione e soprattutto il mantenimento dei requisiti di qualità tanto dei dati tanto delle condizioni del consenso nel suo configurarsi informato, libero, specifico e inequivocabile.

Si delinea uno scenario in cui il soggetto interessato - sotto la spinta di avvenute violazioni dirette o indirette, percepisce preoccupazione per la protezione dei propri dati personali, dispone di misure normative e tecniche per il controllo dei propri dati, ma dicotomicamente manifesta un'attitudine e un comportamento contrari alle aspettative avvalendosi solo marginalmente le misure tecniche di protezione ma soprattutto divulgando dati personali sulla base di un consenso che per quanto sia il principale meccanismo di controllo e di rilascio dei dati personali, permane carente nel ricalibrarsi dinamicamente al variare delle finalità e degli utilizzi.

Quanto premesso ha motivato e orientato il lavoro di ricerca verso la disamina della centralità degli utenti sia nei processi di rilascio e gestione delle informazioni personali sia in quelli della *privacy,* con lo scopo di individuare un modello basato su politiche *users-centric* di supporto ad un *efficace* e *dinamico* controllo del trattamento e della divulgazione dei dati personali in contesti informazionali in cui il mantenimento dei requisiti di qualità tanto dell'informativa quanto dell'autorizzazione al trattamento risultano critici ed inefficaci per la compresenza di una molteplicità di soggetti interessati (*Multiple Subjects Personal Data*) nonché per il subentro – rispetto alle condizioni iniziali, di ulteriori utilizzi, di diverse finalità e quindi di nuove e riformulate vulnerabilità.

L'obiettivo generale del progetto risponde alla determinazione di voler inquadrare l'oggetto della ricerca in coerenza allo scenario regolatorio ricalibrato dal nuovo Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio in vigore dal 24 Maggio 2016; alla ricontestualizzazione del concetto di dato personale, di sfera privata e di *privacy;* e alle diverse misure tecniche.

In conseguenza, l'obiettivo specifico del progetto di ricerca, analizzati contesti informazionali compatibili con schemi di trattamento *Big Data* – trattamento avviato da dati personali rilasciati volontariamente dal soggetto interessato e distinto da un'ampiezza descrittiva del dato tanto quantitativa e che qualitativa – punta a suggerire nuove forme di vulnerabilità e di rischi le cui ricadute possono essere misurate *ex ante* in termini di degrado della qualità dei dati; al contempo, rispetto e a supporto della validità del modello di vulnerabilità proposto, il progetto propone una semplice prova concettuale includente

contromisure *user-centric* basate su politiche di protezione delle informazioni personali di tipo *Sticky Privacy Policies*.

L'obiettivo generale è coperto dai capitoli 1, 2 e 3, quello specifico dai capitoli 4 e 5 così come illustrato al successivo paragrafo 4 - *La Struttura della Tesi*.

3. I CONTRIBUTI DELLA TESI. APPROCCIO E METODOLOGIA.

Le questioni aperte e gli obiettivi posti hanno richiesto una necessaria e imprescindibile configurazione iniziale del progetto di ricerca consistente nell'inquadrare come oggi possano essere concettualizzate la *privacy* e la protezione dei dati personali sulle quali le *disruptive technologies* e gli schemi di trattamento *data intensive* avviati con dati forniti volontariamente dall'utente, oltre ad eliminare la perimetrazione tra la sfera privata e quella pubblica hanno di fatto esercitato una sorta di *evoluzione ontologica.*

I requisiti della *privacy* e della protezione dei dati personali riflettono il differenziarsi della nozione di sfera privata, dilatatasi sotto la spinta delle nuove tecnologie e in risposta ad un mutato ruolo del soggetto interessato. Tecnologie che hanno fin dall'inizio hanno orientato le originarie coordinate legali della *privacy,* configurandola come diritto ad essere *lasciati (da) soli (the right to be let alone)*[23]. La figura che segue è stata prodotta per esemplificare graficamente questa contingente evoluzione.

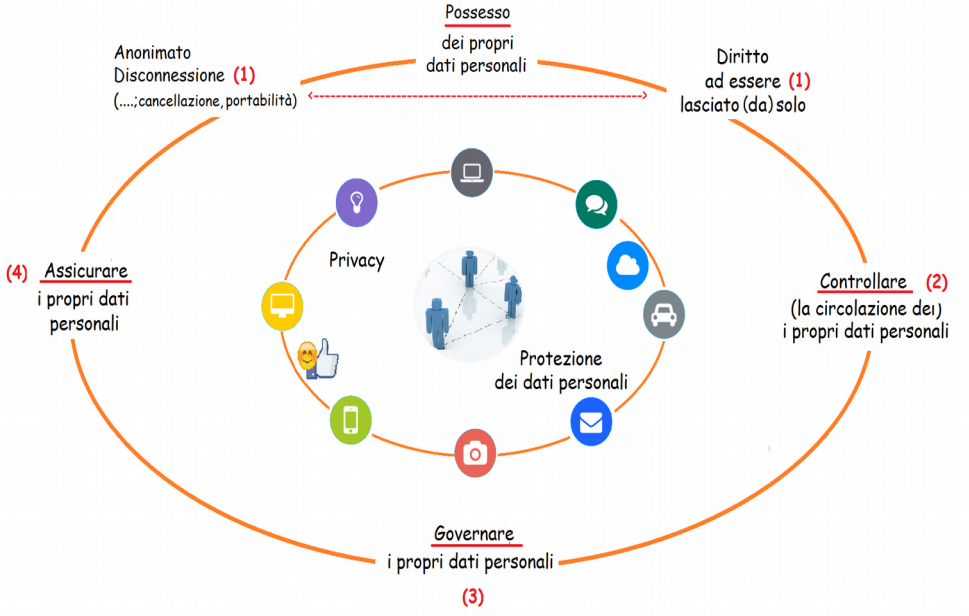


Figura i.1: Evoluzione del concetto di *Privacy* e di protezione dei dati personali

Procedendo in senso orario, viene evidenziato il passaggio da una *privacy* che:

1. riflette il requisito della riservatezza e del possesso individualistico delle proprie informazioni: un presidio esclusivo di una sfera privata ben perimetrata;

[23] Cfr WARREN S., BRANDEIS L., *The Right to Privacy*, in Harvard Law Review, 1890, 4, p. 193-220

2. ad una *privacy* intesa come *protezione dei propri dati personali:* un controllo sulle proprie informazioni - nella loro dinamicità e *libera circolazione;* un controllo che ogni persona può esercitare[24] non solo per *seguire i propri dati ovunque essi si trovino*[25] ma anche per poterli *portare ovunque.* Si passa, quindi e ciclicamente, da un diritto individualistico, statico e limitato (al limite esclusivo e negativo) ad un diritto relazionale, dinamico, allargato (condiviso tra tutti i soggetti interessati e positivo); un diritto che attiene oltre la titolarità di gestione (al limite il possesso) anche il formato e le caratteristiche dei dati personali[26];

3. un controllo che diventa *governo* delle proprie informazioni nella misura un cui *ogni* soggetto interessato diventa utente centrale e consapevole a concorrere – nel modo più semplice possibile e secondo un approccio orizzontale, alla configurazione dei vincoli di raccolta, di successivo trattamento e delle finalità di (ri)utilizzo;

4. infine, una forma di protezione *qualitativa* che sempre più intreccia le prerogative di controllo di tutti i soggetti interessati con le caratteristiche, il significato e la relazione semantica tra i dati; e che assume il significato di *assicurazione* e garanzia se la si considera strumento di salvaguardia della *veridicità* e del *valore* delle proprie informazioni personali.

   Una forma di *assurance* delle informazioni personali intese come *bene prezioso* che l'utente espone in pubblico sotto la duplice spinta posta da un rivoluzionato modo di comunicare e condividere contenuti, e dal desiderio di riaffermare se stesso in un mondo digitale che tendenzialmente affianca alla tipizzazione degli oggetti anche quella delle persone.

In questo contesto il ripristino del *possesso* dei dati personali può essere attuato: *i)* ricorrendo ad un rilascio di informazioni (personali) sempre più sottratto di dati identificativi (e di cui l'anonimizzazione è il limite); *ii)* esercitando un sorta di disconnessione virtuale mediante l'esercizio congiunto dei diritti di cancellazione e portabilità dei dati personali; o *iii)* con una vera e propria disconnessione[27].

Questo passaggio si è rivelato fondamentale per completare la finalizzazione dell'obiettivo principale al quale corrisponde un contributo di carattere concettuale consistente

[24] Art. 1 del CODICE, *Diritto alla protezione dei dati personali.*

[25] STEFANO RODOTÀ, *Il mondo nella rete. Quali i diritti quali i vincoli.* Editori Laterza, cap. 4, pag. 29.

[26] Art. 20 del GDPR, *Diritto alla Portabilità dei Dati*

[27] In argomento cfr: Emanuele Dagnino, ricercatore Adapt «Disconnettersi » è un diritto?, Ottobre 2016 http://job24.ilsole24ore.com/news/Articoli/2016/10/smart-working-dagnino-diritto-disconnessione-video.php?uuid=5fc9be7e-871b-11e6-a440-ad9d3e9fab97&DocRulesView=Libero, Smart working -

nel mettere a sistema, sulla base delle più importanti posizioni rintracciate in letteratura, gli elementi del contesto di riferimento al quale - oltre all'evoluzione del concetto di *privacy,* concorrono: *a)* una profonda rimodulazione della centralità dell'utente rilevabile sia in fase di *disclosure* delle informazioni personali, sia in fase di impostazione delle *preferences* di *privacy; b)* la caratterizzazione del dato personale tanto per la sua funzione identificativa del soggetto interessato, tanto per i requisiti di qualità, tanto per la necessità di un suo ripensamento descrittivo e di formato.

Gli ulteriori contributi della tesi possono essere distinti in uno di carattere analitico e uno di carattere applicativo.

Il primo è connesso a: *a)* illustrare le limitazioni delle azioni regolatorie - sia tecniche che normative, nella misura in cui le prime – distinte in misure di sicurezza, in misure basate su politiche d'uso e in *Privacy Enhancing Technologies* – mancano di un sistema implementativo unitario e comprensivo; e le seconde mantengono un approccio alla protezione dei dati personali di tipo *top-down,* in cui il rafforzamento del principio dell'*accontability* dei titolare e del responsabile non risulta essere stato contro-bilanciato da un parallelo *empowerment* del soggetto interessato; *b)* suggerisce nuove vulnerabilità di *privacy* in contesti distinti da una forte inferenza informativa (quantitativa e qualitativa) e da una pluralità titolari e di soggetti interessati. Queste sono state individuate: nell'asimmetria informativa tra chi produce le informazioni e chi le sfrutta; nella massimizzazione quantitativa dei dati utilizzati; nel mantenimento degli indicatori di qualità del consenso; nel proliferare delle incontrollate finalità di utilizzo; nella perdita di controllo sulle informazioni personali, nell'eccesso di esposizione del soggetto interessato.

Il secondo contributo propone una *Proof of Concept* rispetto e a supporto della validità delle argomentazioni di cui al precedente punto *ii.b.:* utilizza come contesto applicativo l'App *WhatsApp Messenger,* modella la rubrica contatti di un utente *WhatsApp* come un *Personal Data Store* a soggetti multipli *(Multiple Subjects Personal Data Store),* propone un modello implementativo di supporto in cui vengono intersecate le regole d'uso di ogni utente. Nello specifico viene dimostrato: *a)* la carenza di trasparenza e informativa in ragione di ambiguità e lacune rintracciate nel *Privacy Notice* regolatorio esposto da *WhatsApp; b)* l'effettiva ricorrenza di alcune nuove vulnerabilità (asimmetria informativa, eccesso di dei dati personali utilizzati) esemplificandone le relative implicazioni di rischio (perdita di controllo sui dati ed eccesso di esposizione dell'utente) per i dati personali rilasciati e condivise tramite l'App; *c)* quindi, il possibile superamento delle criticità premesse, mediante la scrittura di regole d'uso *user-centric* di tipo *Sticky Privacy Policies*. Questa scelta sfrutta la prerogativa delle *Sticky Privacy Policies* –

quale contenitore di regole di utilizzo definite dall'utente ed integrato ai dati controllati, di poter essere agganciate alla lista contatti di un utente, consentendo a questi di filtrare – in fase di *disclosure,* il rilascio di informazioni personali gestite dall'App mantenendone il controllo durante il successivo utilizzo.

In chiusura viene proposto un set di nuovi descrittori semantici associabili ad altrettante proprietà del dato personale, affinché la modellazione ricavabile supporti, in prospettiva, una ottimale definizione e esecuzione di politiche di *privacy* di tipo *user e data centric.*

Prestando coerenza con la declaratoria delle caratteristiche e delle finalità del curriculum *Informatica giuridica e diritto dell'informatica* del programma di Dottorato di Ricerca in *Diritto e Nuove Tecnologie* XXIX ciclo nell'ambito del quale è stato svolto il lavoro - il profilo della ricerca ha mantenuto una dimensione più tecnica che giuridica optando per una disamina iniziale orientata alle *criticità,* e assumendo come "*stella polare*" il ricalibrato quadro giuridico comunitario - in atto con la promulgazione e l'entrata in vigore del GDPR 2016/679.

Questo approccio ha consentito di cogliere sia le questioni sulla protezione dei dati personali ritenute ancora *aperte* nel GDPR e dalle quali la ricerca ha preso spunto per ragionamenti e ipotesi, sia le indicazioni innovative indirizzanti un deciso cambio di prospettiva le quali si sono rivelate utili per inquadrare e supportare le proposte formulate; tra queste indicazioni rientrano sicuramente la definizione di violazione del dato personale, la caratterizzazione del trattamento in termini di qualità dei dati per la quale si rivelano strumentali il *privacy by design* (intesa come misura di minimizzazione) e la portabilità dei dati (intesa come misura di interoperabilità).

Parimenti si è rivelata importantissima per indirizzo e riscontro la consultazione di alcune *calls* progettuali sul tema inserite nel programma Europeo Horizon 2020[28] e dei pareri emessi dal Gruppo di Lavoro ex. Art. 29[29].

[28] In argomento la pubblicazione della calls H2020 è disponibile su: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens; l'aggiornamento dei progetti finanziati su: http://cordis.europa.eu/programme/rcn/664463_en.html

[29] In argomento la lista dei pareri e delle raccomandazioni prodotte dal Working Party ex art. 29 (oggi Comitato Europeo per la protezione dei dati) sono pubblicati su:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

4. LA STRUTTURA DELLA TESI.

L'elaborato di tesi è organizzato su cinque capitoli oltre appendice e parti accessorie (legenda e abbreviazioni; elenco di tabelle e figure, appendice), raggruppabili logicamente su tre parti:

1. nella prima - ricoperta dal capitolo 1 – *Lo scenario normativo attuale. Questioni aperte,* viene descritto lo scenario normativo attuale evidenziando le principali novità introdotte dall'entrata in vigore del nuovo Regolamento Europeo del 27 Aprile 2016, in compresenza (sino al 24 Maggio 2018) con la Direttiva madre 95/46/CE e con il Decreto Legislativo 30 Giugno 2003 n.196 - codice in materia di protezione dei dati personali. In questo capitolo in particolare sono illustrate le prescrizioni indirizzate ai principi di protezione delle informazioni personali sovrapponibili ai requisiti di tipo *user-centric* e *data-centric;* quindi sono esposti i diritti del soggetto interessato e i principi di qualità dei dati ponendo in chiusura vincoli e questioni aperte;
2. nella seconda parte – ricoperta dai capitoli 2 e 3 - viene illustrato lo stato dell'arte in tema di dato personale e di *privacy,* nonché gli approcci e le contromisure strumentali alla protezione delle informazioni stesse in relazione alle criticità occorrenti. Il capitolo 2 – *Privacy e protezione dei dati personali: pluralità semantiche e criticità*, descrive: le molteplicità semantiche associate allo stesso termine *privacy;* le caratteristiche del dato personale; le criticità e i rischi ricorrenti; gli *stakeholders*, la centralità dell'utente nei processi di rilascio e di trattamento delle informazioni personali. Il capitolo 3 – *Privacy e protezione dei dati personali: le contromisure,* descrive: le contromisure a protezione delle informazioni personali, distinguendo le *Privacy-Enhancing Technologies,* l'anonimizzazione e la pseudonimizzazione; i sistemi di tipo *Privacy Policies-Preferences* ed il framework di *Privacy by Design/Default;*
3. nella terza parte – ricoperta dai capitoli 4 e 5, trova collocazione la trattazione di quegli elementi e di quelle questioni che nel corso del programma di ricerca sono state investigate e ritenute di frontiera. Il capitolo 4 – *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche,* descrive quattro contesti informazionali *data intensive* (*IoT, Apps* per *smart-devices, Big Data* e *Data mining,* Realtà Virtuale e *Data Accretion*) in termini di caratteristiche tecniche e di criticità per il trattamento dei dati personali che in essi trova allocazione; segue la descrizione del nuovo modello di vulnerabilità proposto e le relative tipologie di rischio. Il capitolo 5 – *Progettazione di un modello di supporto a politiche*

di privacy di tipo user e data centric, illustra una *Proof of Concept* rispetto alle argomentazioni descritte nel capitolo quattro.

Vengono infine descritte nuove proprietà associabili all'informazione personale: la *proprietà/il possesso*, la *multi-titolarità dei dati (Multiple Subjects Personal Data)*, il *valore economico* e proposto un set di nuovi descrittori semantici attribuibili al dato personale.

L'elaborato si apre con prefazione e abstract; chiudono conclusioni e sviluppi futuri, appendice e bibliografia.

CAPITOLO 1

LO SCENARIO NORMATIVO ATTUALE. QUESTIONI APERTE.

SOMMARIO: 1. Introduzione – **2.** Dalla Direttiva madre 95/46/CE al Regolamento Generale sulla protezione dei dati (UE) 2016/679. – **3.** Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: *le principali novità.* – **4.** Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: *il soggetto interessato e il dato personale.* – **5.** Questioni aperte.

1. INTRODUZIONE

Il diritto alla protezione dei dati personali è un diritto fondamentale della persona.

Tale diritto è incluso nella Carta dei Diritti Fondamentali dell'Unione Europea (2012/C 326/02)[30], all'art. 8 *Protezione dei dati di carattere personale.*

comma 1) *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;*

comma 2) *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica;*

comma 3) *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

che nel mantenerlo distinto dall'art 7. *Rispetto della vita privata e della vita familiare. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni* - ne riconosce spessore e autonomia.

La distinzione, infatti, non è solo formale. L'art. 7 attiene un diritto *nato materiale*, l'art. 8 un diritto *nato virtuale.* Il primo nel configurare un diritto al *rispetto* della propria vita privata, manifesta una dimensione individualistica, fisica e tangibile; la tutela è statica e la *riservatezza* si misura nell'escludere gli altri da uno spazio perimetrato ritenuto privato. Il secondo configura un diritto alla *protezione* dei dati personali nativamente intangibile, configurato sulla immaterialità del dati; la tutela è dinamica al flusso delle informazioni, il controllo si esplica e si misura nelle regole e nelle modalità di trattamento e di gestione.

Ogni persona ha diritto alla protezione dei dati personali che la riguardano.

Tale diritto è incluso nel Trattato sul funzionamento dell'Unione all'art. 16[31] comma 1).

[30] ex Carta (di Nizza) dei diritto fondamentali dell'Unione Europea, del 7 Dicembre 2000 sostituita dall'entrata in vigore del trattato di Lisbona (01 Dicembre 2009). Con il Trattato di Lisbona e il riconoscimento della vincolatività della Carta dei diritti fondamentali (di Nizza) la protezione dei dati personali è stata formalmente riconosciuta come un diritto fondamentale dell'Unione Europea.

[31] Cfr TFUE TRATTATO SUL FUNZIONAMENTO DELL'UNIONE EUROPEA Art. 16

Il diritto fondamentale alla protezione dei dati personali - già con la Direttiva 95/46/CE del 24 Ottobre 1995[32] e pur nella contingente assenza della Carta dei diritti di Nizza e del Trattato di funzionamento dell'Unione[33], ha rappresentato la base giuridica della normativa europea e nazionale, ispirata ai principi etici di giusto trattamento e di tutela della persona,

La regolamentazione della protezione dei dati personali in Europa si è distinta, sin dall'inizio, per un approccio *generalista* – ovvero assume *un diritto* alla protezione dei dati personali che prescinde e che è indipendente dal settore di applicazione; *centralizzato* e *normativo* – ovvero reso con un unico atto normativo (Direttiva madre, Codice italiano in materia di protezione dei dati personali;[34] e, oggi Regolamento generale sulla protezione dei dati personali (UE) 679/2016[35]).

Un approccio diverso, per esempio, da quello americano o canadese[36] benché ne

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.

Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.

[32] C.d. DIRETTIVA MADRE: Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,* L 281/31, pubblicata nella GUUE del 23.11.1995

[33] Cfr DIRETTIVA 95/46/CE ai considerando:

(1) *considerando che gli obiettivi della Comunità, enunciati nel trattato, come è stato modificato dal trattato sull'Unione europea, consistono nel realizzare un'unione sempre più stretta tra i popoli europei, nell'istituire relazioni più strette tra gli Stati che la Comunità riunisce, nell'assicurare mediante un'azione comune il progresso economico e sociale eliminando le barriere che dividono l'Europa, nel promuovere il miglioramento costante delle condizioni di vita delle sue popolazioni, nel preservare e rafforzare la pace e la libertà e nel promuovere la democrazia basandosi sui diritti fondamentali sanciti dalle costituzioni e dalle leggi degli Stati membri nonché dalla convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali;*

(2) considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui;

(3) considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona;

(10) considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità;

(11) considerando che i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale.

E all'Art. 1 *Oggetto della direttiva* comma1) *Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.*

[34] c.d. CODICE PRIVACY, Decreto Legislativo 30 giugno 2003, n. 196. *Codice in materia di protezione dei dati personali,* pubblicato nella GURI n. 174 del 29 Luglio 2003

[35] c..d. GDPR, Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati* e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) - L 119/34, pubblicato nella GUUE del 4.5.2016.

[36] Settoriale (in cui l'equilibrio tra scambio di dati e protezione è valutato al variare dei settori), decentralizzato (quindi con

condivida l'identico e superiore scopo di proteggere la *privacy* dell'individuo senza limitare o pregiudicare lo scambio e la circolazione di dati e i flussi informativi; fattori, questi, su cui si basa l'attuale e avanzata economia.

Lo scorso 27 Aprile 2016 il Parlamento e il Consiglio Europeo chiudendo un iter legislativo durato 4 anni, approvano:

- ✔ *Il Regolamento (UE) 2016/679 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) - L 119/34*

pubblicato nella Gazzetta Ufficiale dell'Unione del 4 Maggio 2016, entrato in vigore il 25 Maggio dello stesso anno, ma destinato ad avere piena attuazione dal 25 Maggio 2018 data a decorrere dalla quale verrà abrogata la Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995 e, conseguentemente, l'attuale Codice italiano in materia di protezione dei dati personali che recepisce e attua la Direttiva madre. Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri e non richiede una legge di recepimento nazionale. Il Regolamento segna il passaggio da un diritto alla protezione dei dati personali di tipo *nazionale* ad uno di tipo *europeo*.

Il Regolamento (UE) 2016/679 che mantiene l'approccio generalista e centralizzato, eredita dalla Direttiva, consolidandolo, il considerare *il diritto fondamentale alla protezione dei dati personali quale assicurazione per il diritto all'autodeterminazione informativa, e come tale, inserito (a livello europeo) tra i diritti che riguardano la dignità e la libertà della persona*.

Punta ad elevarne la tutela affinché essa si riveli efficace ma al contempo non bloccante l'evoluzione di una società digitale, rispetto alle prospettive e alle opportunità ad essa connesse. Molti degli elementi innovativi del GDPR nascono, infatti, dal realismo con cui il legislatore europeo, nel pensarlo e costruirlo, ha tenuto conto di una società drasticamente nuova fondata sull'espansione illimitata delle informazioni digitali scambiate con velocità e costi inversamente proporzionali, utilizzate in maniera sempre più sofisticata e interconnesse per produrre ulteriori informazioni, nuova conoscenza.

La Direttiva madre e il GDPR sono prodotti normativi di epoche diverse; così come il Codice Italiano nonostante temporalmente interposto tra i due atti e per molti aspetti lungimirante e anticipatorio di quello che sarebbe divenuto il contesto informazionale futuro

pluralità di leggi) e orientato alla de-regolamentazione.

(attuale)[37]. Dalla Direttiva (1995) al Regolamento (2016) è cambiato il mondo, il modo di trattare i dati e le informazioni anche personali: molti strumenti e dispositivi oggi utilizzati non esistevano negli anni di emanazione della Direttiva (smartphone, smart-device, activity tracker), impensabile l'affermazione e la capacità inferenziale di *Big Data* e *Data Mining* che oltre a indirizzare una ricalibratura regolatoria ha evidenziato - per il tramite di pratiche di profilazione sempre più accurate e mirate, il (nuovo) valore economico del dato personale.

Il biennio assegnato dal legislatore europeo tra l'entrata in vigore del GDPR (2016) e la sua piena attuazione (2018) è un tempo ritenuto necessario più per *adottare* il Regolamento in quanto tale che per *adattare* alle sue prescrizioni i compresenti atti nazionali (in Italia il Codice).

Questo elemento e la contestuale approvazione del Regolamento in contingenza dello svolgimento del programma di ricerca (Regolamento che di per se può essere confrontato con la Direttiva più che con il CODICE), ha indotto la scelta di omettere la trattazione specifica del Codice italiano (sebbene inizialmente prevista) - perché ritenuta, se disaminata nel suo complesso, superata dalla contestuale entrata in vigore del Regolamento; ma al contempo optare per intercalarne il richiamo di alcune specifiche disposizioni, ritenute significative sia perché ancora vigenti sia perché rivelatesi sovrapponibili al novellato regolatorio del GDPR.

Il presente capitolo quindi descrive il passaggio dalla Direttiva 95/46/CE al Regolamento generale 679/2016, di quest'ultimo illustra i principali aspetti di novità per focalizzarne la disamina su quelli maggiormente attinenti la tematica di ricerca trattata e concernenti: *i)* gli aspetti di centralità dell'interessato rispetto alla tutela dei suoi diritti e delle sue libertà, nonché gli strumenti (normativi) di controllo di cui dispone per la protezione dei propri dati; e *ii)* le caratteristiche (di qualità) del dato personale che supportano e concorrono a configurare la base giuridica del trattamento sotto il profilo della liceità.

Chiude una disamina delle questioni aperte associabili al ricalibrato quadro normativo, alcune nuove e intrinseche e altre ereditate dal precedente impianto regolatorio.

[37] In argomento si richiamano le disposizioni del CODICE attinenti il passaggio dalle regole di tipo *opt-out* a *opt-in* - volte a legittimare la raccolta subordinatamente alla pre-dichiarata volontà di volerla accettare, mediante tutta l'infrastruttura regolatoria della configurazione e del gestione del consenso art. 23 *Consenso* e art. 24 *Casi nei quali può essere effettuato il trattamento senza consenso;* l'importanza e i vincoli sul trattamento derivanti del principio di minimizzazione dell'utilizzo dei dati personali e dei dati anonimi art.3 *Principio di necessità nel trattamento dei dati* - che nel GDPR diventa la base portante del *Privacy by Design;* nonché la stessa definizione di dato anonimo art. 4 *Definizioni*, comma 1) lettera n) - assunta *di fatto* nel GDPR; nonché tutto l'impianto concernente i diritti azionabili dall'interessato per il controllo sulla circolazione dei propri dati e le relative modalità di esercizio, Art. 7. *Diritto di accesso ai dati personali ed altri diritti*, Art. 8. *Esercizio dei diritti,* Art. 9. *Modalità di esercizio,* Art. 10. *Riscontro all'interessato;* nonché la partecipazione all'esercizio dei poteri di controllo e di intervento dell'interessato anche di una Autorità garante e indipendente.

2. DALLA DIRETTIVA MADRE 95/46/CE AL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (UE) 2016/679.

Il Regolamento generale sulla protezione dei dati personali (UE) 2016/679 benché mantenga analogo impianto definitorio, si colloca tanto in uno scenario informazionale tanto in una prospettiva molto diversi rispetto alla Direttiva 96/46/CE.

Nel 1995 – anno della Direttiva madre, i dati personali *circolavano* nei perimetro delle elaborazioni automatizzate connesse all'utilizzo delle banche dati che per quanto fossero già in grado di implementare collegamento e incrocio tra le informazioni queste operazioni non oltrepassavano la *connessione cablata* tra *mainframe*/terminale piuttosto che tra *data base server*/computer trovando nell'*archivio* istanza applicativa conclusiva. I *personal computer* se già riscontravano affermata diffusione sia domestica che nelle realtà organizzative pubbliche ed in particolare private, non potevano considerarsi strumenti di comunicazione permanendo ancora disconnessi da una rete Internet, che in Italia - dal primo *ping* all'Università di Pisa (1987), per almeno un decennio si sarebbe mantenuta sostanzialmente utilizzata in ambito scientifico e di ricerca. Infine nel 1995 la maggior parte delle persone si scambiava corrispondenza con fax e francobolli; telefonava per lo più con il telefono di casa e quotidianamente leggeva in differita, sui quotidiani cartacei acquistati in edicola, le notizie del giorno prima.

Ne la protezione ne la sicurezza delle informazioni digitali erano questioni percepite con preoccupazione da parte delle persone.

In questo contesto la Direttiva 95/46/CE che si rivela visionaria di quello che sarebbe diventato lo scenario futuro,[38] fonda di fatto la configurazione del diritto alla protezione dei dati personali come diritto all'*autodeterminazione informativa* del soggetto interessato inserendo tale diritto nell'ambito dei diritti che riguardano le libertà e - implicitamente, benché non ne contenga espressamente il termine, la dignità della persona. L'idea del pieno controllo dei dati in capo al soggetto interessato è alla base della Direttiva e si esplica attraverso l'introduzione del paradigma regolatorio del trattamento [informativa-finalità-consenso][39] che pone al centro

[38] Cfr DIRETTIVA 95/46/CE ai considerando:
(4) *considerando che nella Comunità si ricorre sempre più frequentemente al trattamento di dati personali nei vari settori delle attività economiche e sociali; che i progressi registrati dalle tecnologie dell'informazione facilitano notevolmente il trattamento e lo scambio di tali dati;*
(14) *considerando che la presente direttiva dovrebbe applicarsi al trattamento dei dati in forma di suoni e immagini relativi a persone fisiche, vista la notevole evoluzione in corso nella società dell'informazione delle tecniche per captare, trasmettere, manipolare, registrare, conservare o comunicare siffatti dati;*
E all'Art. 33
<....> *La Commissione esaminerà in particolare l'applicazione della presente direttiva al trattamento dei dati sotto forma di suoni o immagini relativi a persone fisiche e presenterà le eventuali proposte necessarie, tenuto conto dell'evoluzione della tecnologia dell'informazione e alla luce dei progressi della società dell'informazione.*

[39] Cfr DIRETTIVA 95/46/CE ai considerando:

il soggetto interessato per il tramite di tutta una serie di diritti da questi azionabili (di accesso, opposizione, rettifica, cancellazione) volti a verificare e mantenere la liceità e la legittimità del trattamento[40]; un paradigma che negli anni successivi troverà pieno recepimento e attuazione nel Codice Italiano, nonché perfezionamento in relazione ai diversi tipi di dati personali e di trattamento.

Il decennio successivo sino al 2005 - periodo in cui i dati personali *circolano* nella rete

---

(28) *considerando che qualsivoglia trattamento di dati personali deve essere eseguito lealmente e lecitamente nei confronti delle persone interessate; che esso deve in particolare avere per oggetto dati adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite; che tali finalità devono essere esplicite e legittime e specificate al momento della raccolta dei dati; che le finalità dei trattamenti successivi alla raccolta non possono essere incompatibili con quelle originariamente specificate;*

(30) *considerando che, per essere lecito, il trattamento di dati personali deve essere inoltre basato sul consenso della persona interessata oppure deve essere necessario ai fini della conclusione o dell'esecuzione di un contratto vincolante per la persona interessata, oppure deve essere previsto dalla legge, per l'esecuzione* di *un compito nell'interesse pubblico o per l'esercizio dell'autorità pubblica, o nell'interesse legittimo di un singolo individuo, a condizione che gli interessi o i diritti e le libertà della persona interessata non abbiano la prevalenza; che, segnatamente, per garantire un equilibrio degli interessi in causa, pur assicurando una concorrenza effettiva, gli Stati membri possono precisare le condizioni alle quali dati personali possono essere usati e comunicati a terzi nell'ambito di attività lecite di gestione corrente delle imprese o di altri organismi; che essi possono parimenti precisare le condizioni alle quali può essere effettuata la comunicazione a terzi di dati personali a fini di prospezione, sia che si tratti di invio di materiale pubblicitario che di invio di materiale promosso da un'associazione a scopo benefico o da altre associazioni o fondazioni, ad esempio a carattere politico, nel rispetto delle disposizioni volte a consentire alle persone interessate di opporsi senza dover fornire una motivazione e senza spese al trattamento dei dati che le riguardano;*

(38) *considerando che il trattamento leale dei dati presuppone che le persone interessate possano conoscere l'esistenza del trattamento e disporre, quando i dati che le riguardano sono forniti direttamente da loro, di un'informazione effettiva e completa in merito alle circostanze della raccolta;*

(39) *considerando che alcuni trattamenti riguardano dati che il responsabile non ha raccolto direttamente presso la persona interessata; che è peraltro possibile che taluni dati siano legittimamente comunicati a terzi anche se tale comunicazione non era stata prevista all'atto della raccolta dei dati presso la persona interessata; che, in tutti questi casi, la persona interessata deve essere informata al momento della registrazione dei dati o al massimo quando essi sono comunicati per la prima volta a terzi;*

(48) *considerando che la notificazione all'autorità di controllo ha lo scopo di dare pubblicità alle finalità del trattamento ed alle sul principali caratteristiche, per consentirne il controllo secondo le norme nazionali di attuazione della presente direttiva;*

SEZIONE IV, *Informazione della persona interessata*

Art. 10 I*nformazione in caso di raccolta dei dati presso la persona interessata,* Art.11 *Informazione in caso di dati non raccolti presso la persona interessata*

<...>

a) *l'identità del responsabile del trattamento ed eventualmente del suo rappresentante;* b) *le finalità del trattamento cui sono destinati i dati;*

[40] Cfr DIRETTIVA 95/46/CE ai considerando:

(41) *considerando che una persona deve godere del diritto d'accesso ai dati che la riguardano e che sono oggetto di trattamento, per poter verificare, in particolare, la loro esattezza e la liceità del trattamento; che, per le stesse ragioni, le persone devono avere inoltre il diritto di conoscere la logica su cui si basa il trattamento automatizzato dei dati che le riguardano, perlomeno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1; che tale diritto deve lasciare impregiudicati il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software; che ciò non dovrebbe comunque tradursi nel rifiuto di fornire qualsiasi informazione alla persona interessata;*

(42) *considerando che gli Stati membri possono, a beneficio della persona interessata o a tutela dei diritti e delle libertà altrui, limitare il diritto d'accesso e d'informazione; che possono, ad esempio, precisare che l'accesso ai dati medici è possibile soltanto per il tramite del personale sanitario;*

(43) *considerando che gli Stati membri possono altresì imporre analoghe restrizioni al diritto di accesso e di informazione e ad alcuni obblighi del responsabile del trattamento nella misura in cui tali restrizioni siano necessarie per salvaguardare, ad esempio, la sicurezza nazionale, la difesa, la pubblica sicurezza, importanti interessi economici o finanziari di uno Stato membro o dell'Unione, nonché per indagini e procedimenti penali e in caso di violazioni dell'etica delle professioni regolamentate; che occorre elencare, a titolo di deroghe e restrizioni, i compiti di controllo, di indagine o di regolamentazione necessari negli ultimi tre settori suindicati relativamente alla pubblica sicurezza, agli interessi economici o finanziari e alla repressione penale; che l'elenco dei compiti relativi a questi tre settori lascia impregiudicata la legittimità delle deroghe e restrizioni giustificate da ragioni di sicurezza di Stato e di difesa;*

(45) *considerando che, in caso di dati che potrebbero essere oggetto di un trattamento lecito per ragioni di interesse pubblico, di esercizio dell'autorità pubblica o di interesse legittimo di un singolo, qualsiasi persona interessata dovrebbe comunque avere il diritto, per ragioni preminenti e legittime connesse alla sua situazione particolare, di opporsi al trattamento dei dati che la riguardano; che gli Stati membri hanno tuttavia la facoltà di prevedere disposizioni nazionali contrarie;*

SEZIONE I, *I principi relativi alla qualità dei dati*

Art. 6 comma 1) *Gli Stati membri dispongono che i dati personali devono essere:*

pubblica e in cui ricade l'emanazione del Codice *privacy* italiano (2003), segna lo sviluppo e l'affermazione su larga scala della telefonia mobile ed in particolare di Internet (Web 1.0) – tecnologie e servizi che inizialmente incidono sulla vita delle persone in maniera autonoma e distinta. Internet e il Web 1.0 - interconnettendo a velocità sempre crescenti i *personal computer,* veicolano lo scambio, la condivisione e la pubblicazione di informazioni digitali, qualificandone l'utente (la persona interessata) come il principale produttore. In questi anni le persone comunicano per posta elettronica, via chat, attraverso *web application* centralizzate come forum e le mailing-list; oltre che con le modalità offerte dalla telefonia mobile: voce e messaggistica (*SMS - Short Message Service, MMS – Multimedia Message Service*); gli utenti cominciano ad apprezzare la convenienza di fare acquisti *on-line;* fruiscono di servizi di ricerca delle informazioni che comunque si mantengono sintattici (basati cioè sull'incrocio di parole chiavi) asincroni/informativi/localizzati.

In questo periodo - che tra l'altro registra una forte spinta in ambito pubblico verso la digitalizzazione dei processi e dei servizi gestiti e offerti dalla pubblica amministrazione[41], al sempre maggiore utilizzo della rete pubblica si affianca la conoscenza della sua intrinseca insicurezza per i dati che veicola, rispetto ai requisiti di riservatezza, integrità e autenticità.

---

a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati; <....>

SEZIONE II, *Principi relativi alla legittimazione del trattamento dei dati*
Art. 7 *Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando*: *a) la persona interessata ha manifestato il proprio consenso in maniera inequivocabile <....>*

SEZIONE V, *Diritto di accesso ai dati da parte della persona interessata*
Art. 12 *Diritto di accesso*
Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:
a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi:
- la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati;
- la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati;
- la conoscenza della logica applicata nei trattamenti automatizzati dei dati che lo interessano, per lo meno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1;
b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati;
c) la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

SEZIONE VII, *Diritto di opposizione della persona interessata*
Art. 14 *Diritto di opposizione della persona interessata*
Art. 15 *Decisioni individuali automatizzate*
comma 1) *Gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc.*

[41] In argomento si richiamano a mero titolo di esempio, l'emanazione dei primi atti normativi in materia di documento informatico, firma digitale, protocollo informatico che convergevano nella prima formulazione del codice dell'amministrazione digitale cn D.lgs. 7 marzo 2005 n. 82, Codice dell'amministrazione digitale, pubblicato in G.U. n. 112 del 16.05.2005 e successive modifiche.

La *privacy* ma in particolare la *sicurezza* delle informazioni e dei sistemi diventano questioni importanti tanto per le aziende tanto per gli utenti[42].

Le parole chiavi rappresentative possono essere mutuate da alcune definizioni introdotte nel Codice *privacy* italiano che contemperando realismo e lungimiranza coglie la portata innovativa del tempo: *"banca di dati"; "comunicazione elettronica", "reti di comunicazione elettronica", "rete pubblica di comunicazioni", "servizio di comunicazione elettronica", "utente", "dati relativi al traffico", "posta elettronica"; "misure minime", "strumenti elettronici", "autenticazione informatica", "profilo di autorizzazione", "sistema di autorizzazione", "violazione di dati personali".*[43]

Oggi, a vent'anni di distanza la società vive in una dimensione proiettata verso una totale digitalizzazione, *sincronizzata, delocalizzata, correlata* in cui il continuo trattamento digitalizzato delle informazioni e dei dati personali è divenuto l'asse portante di ogni relazione interpersonale con processi informativi di tipo *A2A*[44] e di tipo *A4A*[45]*,* che operano *wireless,* pervasivi e distribuiti. Oltre alla tecnologia *wireless* le innovazioni che hanno definito questo scenario sono soprattutto il *Web 2.0* che ha permesso l'utilizzo di massa della rete per scambiare e soprattutto produrre informazioni, contenuti e media originando la diffusione dei *social;* il *cloud* e il *mobile* che con la potenza di connessione, la robustezza dello *storage* e la flessibilità delle *apps* supportano la produzione dei dati personali, la possibilità di acquisirli, conservarli, trattarli e incrociarli in maniera sempre più efficiente, aprendo e affermando il fenomeno dei *Big Data* distinto dalle 3+3 V[46]; *Big Data,* il cui volume di dati è ulteriormente incrementato da quelli prodotti dagli algoritmi dell'Intelligenza Artificiale e dai sensori dell'*IoT* (*IoT, Internet of Things*).

Tutto ciò ha configurato sistemi di analisi delle informazioni sempre più raffinati e accurati – *Data Mining* e *Data Anlytics,* che alla funzionalità di *cercare* e *produrre* informazioni in rete – che rimane una attività *lato utente* e svolta dal soggetto interessato, hanno affiancato quella di *inferire* dati da dati e *dedurre* informazioni da informazioni, una attività che, invece, si mantiene configurata *lato cloud, lato OTT*[47], prerogativa cioè di chi raccoglie i dati, gestisce gli

[42] In questo frangente gli utenti, in linea di massima, percepiscono e misurano l'insicurezza delle reti pubbliche in termini di furto di qualcosa liberamente disponibile in rete (credenziali, password, documenti, immagini) o all'intrusione in una sfera privata ancora ben localizzata.

[43] Cfr CODICE art. 4 *Definizioni* comma 1) lettera p); comma 2) lettera a) c) d) e) g) h) m); comma 3) a) b) c) e) f) g) g-bis.

[44] Con l'espressione *A2A - Anything to Anything*, si fa riferimento a ogni cosa che è connessa e che comunica con ogni altra in maniera distribuita.

[45] Con l'espressione *A4A - Anywhere for Anytime*, si fa riferimento all'interconnessione senza soluzione di continuità e di luogo; continua, pervasiva e capillare.

[46] Le caratteristiche dei *Big Data,* al cui approfondimento per i rischi attinenti i dati personali e le implicazioni sulla loro protezione si rimanda al capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche,* sono schematizzate in letteratura con il paradigma delle 3 V: *Volume, Velocità e Varietà.* Alle quali oggi appare coerente e rappresentativo aggiungere: *Variabilità, Veridicità, Valore.*

[47] *OTT* è l'acronimo di *Over The Top;* riguarda imprese che forniscono servizi e applicazioni che consentono la vendita di

algoritmi di analisi, sfrutta le informazioni, ne deduce di nuove.

In questo nuovo scenario non poteva non cambiare l'approccio per assicurare un efficace protezione dei dati personali, rendendosi al contempo necessario un superamento della Direttiva non tanto per il suo contenuto quanto come tipologia di strumento giuridico.

La base giuridica del Regolamento è rappresentata dall'art. 8 della Carta dei Diritti fondamentali dell'Unione Europea e dall'art. 16 del Trattato di Funzionamento dell'Unione Europea; il Regolamento quindi attua e consolida un diritto fondamentale – quello della protezione dei dati personali, introdotto e già ampiamente attuato dalla Direttiva (ed in Italia successivamente dal Codice) pur nell'allora contingente assenza delle norme che lo qualificano come diritto fondamentale.

In tal senso il Regolamento si collega alla Direttiva, non la invalida e ne eredita (rafforzandolo) il principio portante; tuttavia ne palesa la necessità di un superamento in ragione della sua inadeguatezza come strumento giuridico rivelatosi inefficace nell'eliminare tanto la frammentazione della protezione dei dati personali nel territorio dell'Unione tanto l'incertezza giuridica. Questo aspetto è ben esposto dal considerando 11 del GDPR: *un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.*

Il porre sulla stessa dimensione diritti, obblighi e poteri di controllo registra il proiettarsi del regolamento verso una prospettiva pubblicistica e non solo civilistica[48].

Nel Regolamento avviene un rilevante rovesciamento di caratterizzazione passando da un apparato normativo tutto incentrato sui diritti dell'interessato ad uno complementare: *i)* basato sui doveri del titolare e del responsabile, *ii)* con un rafforzamento dell'Autorità di Controllo, ed *iii)* in cui alla centralità del soggetto interessato - rimasta sostanzialmente immutata, si introduce e affianca la centralità del dato personale e del trattamento stesso.

Direttiva e Codice Italiano hanno costruito il diritto alla protezione dei dati personali

prodotti o
di pubblicità connessi ai contenuti trasmessi e ad altri tipi di servizi forniti come, ad esempio, i motori di ricerca. Queste imprese che comprendono tra gli altri anche Google Inc., Apple Inc., Facebook Inc., sono definite Over The Top perché per trasmettere i contenuti non si servono di strutture proprie ma delle reti di telecomunicazioni e quindi *operano sopra le reti.*

[48] Cft Atti dell'intervento titolato: *La privacy e il diritto europeo alla protezione dei dati personali, dalla Direttiva 95/46 al nuovo Regolamento europeo,* tenuto dal prof. Franco Pizzatti, Costituzionalista ex Garante per la protezione dei dati personali Italiana, al PrivacyDay Forum organizzato da FederPrivacy e tenutosi a Roma il 13 Ottobre 2016.

basandolo tutto sull'autodeterminazione informativa del soggetto interessato al quale i dati personali concernono; e ciò in definitiva per evitare che venga svuotata la stessa libertà della persona intesa come libertà da ogni controllo illecito.

Il nuovo Regolamento Europeo eredita questa costruzione, mantenendola in ragione del nuovo scenario informazionale ogni qualvolta le informazioni personali che sono richieste o volontariamente rilasciate dal soggetto interessato vengono utilizzate per finalità diverse da quelle per quali inizialmente raccolte, per consentire attraverso incroci e analisi consentire di scoprire aspetti della vita, delle attività, o della personalità che non si vuole rendere pubblici.

Il cambio di prospettiva tra Direttiva e Regolamento può essere inquadrato sui seguenti punti ai quali si agganciano le principali novità introdotte dal GDPR[49]:

1. *il passaggio da un diritto nazionale a un diritto europeo.* La Direttiva è un atto normativo di armonizzazione, la cui attuazione passa attraverso leggi di recepimento nazionali. Ciò ha configurato un diritto alla protezione dei dati personali di tipo *nazionale* – in Italia attuato con il Codice, Decreto Legislativo 196/2003 – ponendo la Direttiva stessa in subordine. Dal 25 Maggio 2018 quando il Regolamento Europeo avrà (piena) attuazione e la Direttiva e il Codice abrogati, il ricorso alla legislazione nazionale sarà residuale e non centrale, esso riguarderà le parti attuative o interstiziali del Regolamento e quelle in cui rinvia ai singoli Stati discipline specifiche[50]; comunque la normativa base sarà quella del Regolamento.

Il legislatore europeo ha inteso superare il carattere *nazionale* della Direttiva attribuendo medesimi diritti e medesime pretese a tutti i cittadini dell'Unione, ponendo sullo stesso piano tutti i paesi europei, perseguendo al contempo l'assicurazione di una maggiore certezza del diritto sull'intero territorio comunitario[51].

La scelta quindi di un atto normativo unico, strutturato e completo punta quindi ad uniformare il diritto dei paesi europei, nonostante permangano disposizioni di rinvio alle

[49] Con riferimento alle quali si rimanda al successivo paragrafo 1.3: *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: le principali novità.*

[50] Cfr GDPR Capo IX *Disposizioni relative a specifiche situazioni di trattamento*

[51] Cfr considerando 11)P*er assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni. Inoltre, le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione (1).*

legislazioni derogatorie dei singoli Stati.[52]

Da qui la scelta di abbandonare la precedente impostazione posta dalle Direttive di armonizzazione - una determinazione sulla quale oltre al mutato contesto informazionale e alle limitazioni in ordine alla frammentazione e all'incertezza del diritto - ha anche pesato il fatto che con il Trattato di Lisbona e il riconoscimento della vincolatività della Carta di Nizza, la protezione dei dati personali è stata definitivamente riconosciuta come diritto fondamentale della persona nell'intero territorio dell'Unione.

2. *il passaggio da un diritto individuale/assoluto a un diritto relazionale/sociale,* in cui meglio si evidenzia la differenza di impostazione tra i due atti regolatori; ciò trova efficace rilievo nel confronto dei due considerando: il 2) della Direttiva - *i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui*; e il considerando 4) del Regolamento - *Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali* <...>. Nonostante la base giuridica del Regolamento rimangano l'art. 7 della Carta di Nizza e l'art. 8 del TFUE e venga mantenuto il diritto alla protezione dei dati personali come diritto fondamentale, questo non è più una prerogativa assoluta. Sulla visione individualista prevale, quindi,

[52] Cfr GDPR considerando 10) *Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.*

Considerando 129) *Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento.* <...>

quella sociale inserita in un bilanciamento di equilibrio con gli altri diritti fondamentali[53].

Il Regolamento, quindi, - anche in ragione dei cambiamenti della società incisi dall'impatto dirompente delle nuove tecnologie[54], supera il carattere *individualistico* della Direttiva, perché considera il diritto fondamentale della persona alla protezione dei dati personali come un fatto sociale, un interesse pubblico (europeo) e non solo individuale; la protezione dei dati personali non è circoscritta alla tutela della persona ma si estende alla società alla quale essa appartiene.

3. *il passaggio da una logica di tutela formale ad una sostanziale.* La Direttiva ha tutelato il diritto fondamentale alla protezione dei dati personali - esplicitato come diritto all'autodeterminazione informativa, da una prospettiva primariamente di carattere *individualistico* e *nazionale;* con un approccio *garantistico* dei diritti e delle tutele individuali reso prevalentemente per il tramite di adempimenti *formali.* Di contro, su quest'ultimo aspetto, il Regolamento – che mantiene il principo di finalità come elemento fondante la legittimità dei trattamenti, il consenso e i diritti azionabili dall'interessato come strumenti di controllo fondamentali, sposta gli adempimenti su una dimensione normativa fortemente *sostanziale* – tutto incentrata sul titolare del trattamento (controller) non più chiamato solo a esibire una serie di adempimenti formali, ma a perseguire e comprovarne l'esito del rispetto sostanziale dei principi cardine del sistema: la liceità del trattamento dei dati, la sua correttezza e la sua trasparenza.

   Al contempo il nuovo Regolamento affronta il nuovo quadro tecnologico con il realismo necessario a gestire le criticità connesse al *differenziarsi delle finalità* e al mantenere, nel tempo, un *consenso di qualità.*[55]

L'implicazione attesa è che dovrebbe potersi superare l'idea di ridurre la *privacy* e la protezione dei dati personali a meri formalismi burocratici legati alla c.d. *firmetta per la privacy;* al contempo poter abbattere ingannevoli preconcetti sull'impossibilità di difendere i propri dati personali da

[53] Cft Atti dell'intervento titolato: *La privacy e il diritto europeo alla protezione dei dati personali, dalla Direttiva 95/46 al nuovo Regolamento europeo,* tenuto dal prof. Franco Pizzatti, Costituzionalista ex Garante per la protezione dei dati personali Italiana, al PrivacyDay Forum organizzato da FederPrivacy e tenutosi a Roma il 13 Ottobre 2016.

[54] Sull'argomento il riferimento alle *Internet disruptive technologies* con le quali si intende raggruppare l'insieme delle tecnologie (interconnesse in rete) di rivoluzionario e al limite destabilizzante impatto innovativo: *Internet of Things, Cloud Computing, Mobile, Robotics,* distinte dallo scambio continuo e massivo di grandi volumi di dati che diventano dominio informativo di Big Data e Data Mining.
In argomento cfr http://www.intelligenthq.com/technology/12-disruptive-technologies/

[55] Questione, questa, che assume un'importanza fondamentale e saliente se si considerano i trattamenti sui dati personali posti in essere con tecniche di Big Data i quali intrinsecamente presentano una pluralità illimitata di finalità. A meno che i dati personali oggetto di trattamento Big Data non siano stati preventivamente anonimizzati e quindi in ragione del considerando 26) del Regolamento ad esso non soggetti, non sarebbero possibili, almeno in linea di principio, trattamenti *nonimi* che perseguono finalità diverse da quelle sulle quali gli interessati hanno fornito il loro consenso informato ed esplicito o che non rientrano tra quelle per le quali sussistano previsioni legislative specifiche derogatorie l'assenza di consenso. Questo argomento verrà in dettaglio trattato nel capitolo 3, paragrafo 2.1 - *L'anonimato e la protezione dei dati personali* e nel capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.*

indebiti trattamenti, comprendere con maggiore consapevolezza i limiti delle tecnologie, individuarne e gestirne *preventivamente* i rischi.

Da questa breve analisi si comprende come la portata del GDPR oltrepassi la diversa fonte utilizzata: il Regolamento muta la prospettiva di fondo in cui si colloca la protezione dei dati personali soprattutto in ordine alle rinnovate e accresciute responsabilità del titolare e del responsabile – configurabili in una vera e propria *assunzione di rischio,* e alle implicazioni attinenti la progettazione del trattamento nel suo insieme, la valutazione *a priori* dell'impatto e dei rischi che questo comporta per i diritti e le libertà delle persone, l'adozione di adeguate e preventive misure organizzative e tecniche ivi incluse quelle di sicurezza che soddisfino i requisiti del regolamento e garantiscano la tutela dei diritti dell'interessato.

3. IL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (UE) 2016/679: *LE PRINCIPALI NOVITÀ.*

Le principali novità introdotte dal Regolamento europeo vanno inquadrate nella considerazione che la se Direttiva madre e – in Italia, il Codice *privacy* sono stati i *costruttori* del diritto fondamentale alla protezione dei dati personali inteso come diritto all'autodeterminazione informativa, il nuovo Regolamento assolve invece ad una funzione *consolidatrice* di tale diritto.

Le novità introdotte dal GDPR possono essere racchiuse in tre categorie tematiche[56], rappresentanti altrettanti sfide: *i)* i *diritti* - il Regolamento per un verso consolida il previgente quadro dei diritti e delle garanzie e ne introducendone di nuovi: il diritto fondamentale alla protezione dei dati personali e del controllo delle proprie informazioni ne risulta rafforzato; *ii)* i *doveri* – aspetto speculare ai diritti e attinenti l'*accountability,* ovvero l'accresciuta responsabilizzazione del titolare del trattamento; e *iii)* la *cooperazione* – tra le Autorità Nazionali di controllo chiamate a svolgere un accresciuto ruolo regolatorio soprattutto in sede di valutazione di impatto di nuovi trattamenti, di valutazione della gravità delle violazioni e della conseguente notifica all'interessato[57]; quindi una cooperazione che si esplica in termini di *governance,* di rafforzamento dei poteri di *vigilanza e controllo* e del *sistema sanzionatorio.*

Per quanto attiene il consolidamento dei *diritti* è possibile evidenziare:

1. una vera e propria introduzione dell'*istituto del consenso esplicito* che – all'art. 4 *Definizioni* comma 11) viene definito come: *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento* - e all'art. 7 *Condizioni per il consenso* viene declinato al comma 2) *Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante;* e al

[56] In argomento ed in particolare sull'esposizione di un quadro di sistema delle principali novità introdotte dal Regolamento 679/2016 si indicano gli atti dell'intervento titolato: *Regolamento UE, la sfida della nuova privacy è già iniziata,* tenuto della prof.ssa Licia Califano, componente dall'Autorità Garante per la protezione dei dati personali Italiana, al PrivacyDay Forum organizzato da FederPrivacy e tenutosi a Roma il 13 Ottobre 2016.

[57] Cfr GDPR art. 35 *Valutazione d'impatto sulla protezione dei dati* comma 4) *L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.* comma 5) *L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.*

comma 3) *L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.*

Una disciplina giuridica quindi, con garanzie molto forti, più stringente sotto il profilo della caratterizzazione della scelta libera che si collega e attua tra l'altro con la possibilità di revoca (cfr passaggi sottolineati che precedono). La definizione inoltre estende le preesistenti caratteristiche di qualità del consenso ereditate dalla Direttiva (*consenso libero, esplicito, informato*) ampliandole con il requisito di *inequivocabilità;*

2. il rafforzamento del potere di scelta degli interessati che non può non prescindere da una effettiva trasparenza nell'esposizione delle caratteristiche dei trattamenti che si porranno in essere. Il Regolamento all'art. 13[58] *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato* e all' art. 14[59] *Informazioni da fornire qualora i dati*

[58] Cfr GDPR Sezione 2 *Informazione e accesso ai dati personali* Art. 13 *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*
1.*In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:*
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f)ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. *In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:*
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3.*Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.*
4.*I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.*

[59] Cfr GDPR Sezione 2 *Informazione e accesso ai dati personali* Art.. 14 *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*
1.*Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:*
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

personali non siano stati ottenuti presso l'interessato punta in maniera precisa e marcata sulla funzione informativa declinando il catalogo delle informazioni da fornire all'interessato. La combinazione del consenso esplicito e di qualità con l'informativa rappresentano il perimetro definitorio fondamentale per la costruzione del diritto alla protezione dei dati personali inteso come diritto all'autodeterminazione informativa.

3. La possibilità di distinguere tra i diritti azionabili dall'interessato: *i)* quelli strumentali all'esplicitazione del controllo sulle proprie informazioni personali e al mantenimento dei requisiti di qualità del consenso (cfr considerando 58-73 art. 12-23 del Regolamento); nel nuovo Regolamento essi vengono sostanzialmente riaffermati e

---

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
d) le categorie di dati personali in questione;
e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f)ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2.*Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:*
a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
e) il diritto di proporre reclamo a un'autorità di controllo;
f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3.*Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:*
a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4.*Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.*
5.*I paragrafi da 1 a 4 non si applicano se e nella misura in cui:*
a) l'interessato dispone già delle informazioni;
b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

riproposti rispetto alla Direttiva e al Codice *privacy* italiano e attengono il diritto di accesso, di rettifica, di cancellazione, di opposizione e di limitazione, quest'ultimo in un'accezione diversa dal previgente diritto che lo connotava come possibilità di chiedere il blocco dei dati; *ii)* il diritto di portabilità dei dati (cfr considerando 68, 73 art. 13, 20 del Regolamento); *iii)* il diritto di opposizione ad attività di profilazione (cfr considerando 70-73 art. 21-23 del Regolamento); *iv)* il diritto all'oblio (cfr considerando 65, 66 e art. 17 del Regolamento).

Le prime tre categorie saranno trattati nel successivo paragrafo 4. *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: il soggetto interessato e il dato personale.*

Il diritto all'oblio rappresenta la positivizzazione della sentenza *Google Spain*[60]*,* amplia la sua originale connotazione di diritto alla de-indicizzazione per diventare qualcosa di più complesso: l'obiettivo del legislatore è quello di estendere la sua applicazione ad ambiti diversi dal trattamento di informazioni effettuato dai motori di ricerca, quali ad esempio editori di testate Web oppure ai trattamenti effettuati dalle Pubbliche Amministrazioni che assolvono agli obblighi di trasparenza mediante pubblicazione di informazioni *on-line*.

In merito alla seconda linea di novità e di sfida introdotta dal Regolamento, quella dei *doveri* essa si collega alla positivizzazione del principio di *accontability* (responsabilizzazione) che diventa una vera e propria *assunzione di rischio,* volta ad uscire dalla logica del mero adempimento formale degli obblighi di legge.

L'intendimento del legislatore europeo è quello di porre chi tratta i dati personali - titolari e responsabili di trattamento, responsabili designati e responsabili della protezione dei dati personali, nella logica di ridurre i rischi di operazioni non consentite o comunque non conformi, quindi di spingere il titolare e il responsabile del trattamento a comportamenti virtuosi; questo se per un verso implica un certo investimento di partenza – connesso agli

[60] Attiene la sentenza con la quale la Corte di Giustizia dell'Unione europea si è pronunciata, in data 13 maggio 2014, in relazione al caso Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González (causa C−131/12).
All'origine della vicenda vi è una richiesta con la quale un cittadino spagnolo aveva cercato di ottenere, prima dal gestore del sito e poi da Google, la rimozione di alcuni dati personali pubblicati su un articolo di giornale ritenuti non più attuali. Su ricorso dell'interessato, l'Agencia Española de Protección de Datos (AEPD) (l'autorità spagnola per la protezione dei dati personali), aveva ordinato a Google di rimuovere i dati in questione dai risultati generati attraverso il motore di ricerca. Google aveva rifiutato di ottemperare alla richiesta rilevando, tra l'altro, come l'intervento imposto dall'AEPD potesse configurare un'indebita compromissione della libertà di espressione dei gestori di siti Internet. La Corte suprema spagnola (Audiencia Nacional), investita dell'appello contro il provvedimento dell'AEPD, sollevava pertanto di fronte alla Corte di Giustizia alcune questioni pregiudiziali relative (i) all'applicabilità della Direttiva 95/46/CE sulla protezione dei dati personali a fornitori di servizi come Google e (ii) al cd. "diritto all'oblio" dei soggetti cui i dati personali si riferiscono.
Il caso e la sentenza possono essere consultati in versione integrale alla seguente risorsa:
http://curia.europa.eu/juris/document/document.jsf?
text=&docid=152065&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=102401

adempimenti *by design* e *by default* delle misure tanto tecniche e organizzative tanto di sicurezza, alla valutazione dell'impatto del trattamento e dei rischi ad esso connesse, alla nomina del responsabile della protezione dei dati, è pur vero che esso ritorna sotto forma di risparmio nel breve e medio periodo in termini di benefici per gli interessati resi più certi della correttezza del trattamento. La positivizzazione del principio di responsabilizzazione del titolare si esplica sui seguenti aspetti:

1. le accresciute e mutate responsabilità del titolare e del responsabile del trattamento dei dati personali declinate in particolare negli art.24[61] *Responsabilità del titolare del trattamento*, art. 25[62] *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita,* e art. 28 *Responsabile del trattamento* che assegna ai responsabili gli stessi doveri dei titolari per quanto attiene l'adozione di misure tecniche e organizzative adeguate a garantire che i trattamenti soddisfino i requisiti previsti dal Regolamento e assicurino una adeguata tutela dell'interessato (cfr considerando 74-77, 79-81, art. 4, 24, 27, 28, 29 del Regolamento). Il titolare del trattamento e - in una logica solidale anche il responsabile per il raccordo dell'art. 28, deve *mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento,* tenendo conto *della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche;* inoltre le misure devono essere *riesaminate e aggiornate qualora necessario.* Questi passaggi contengono l'essenza della positivizzazione del principio di *accountabiliy* con un salto di qualità della responsabilità del titolare e del responsabile

[61] Cfr GDPR Sezione 1 *Obblighi generali*
Art. 24 R*esponsabilità del titolare del trattamento*
1.T*enuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche,* ***il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.***
2.S*e ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.*
3.*L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.*

[62] Cfr GDPR Sezione 1 *Obblighi generali*
Art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*
1.T*enendo 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.U*n 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.*

molto significativa; entrambi non rispondono più a meri adempimenti di conformità, la loro responsabilità si configura flessibile, dinamica, dipendente dalle caratteristiche del trattamento e dalle implicazioni che questo comporta; ma l'aspetto molto più significativo è che essi devono sono tenuti a dimostrare e a comprovare di avere effettivamente adottato le *misure tecniche e organizzative adeguate* <...>. Una responsabilità sostanziale rispetto alla quale risulta fondamentale l'analisi dei rischi per i diritti e le libertà delle persone derivanti dal trattamento, a sua volta strumentale per l'individuazione e l'adozione delle misure di sicurezza.

La responsabilità del titolare e del responsabile attiene sia il garantire la conformità del trattamento ai principi del Regolamento sia il valutare la probabilità del rischio e la misura di gravità per i diritti e le libertà dell'interessato.

2. la misura della rivalutata e accresciuta responsabilizzazione del titolare si rileva nel comma 4 dell'art. 6 *Liceità del trattamento*[63]; una disposizione che racchiude tutta la portata innovativa del Regolamento, per effetto della quale: in assenza di rinnovato consenso dell'interessato, viene posta in capo al titolare la responsabilità di valutare le condizioni di compatibilità sulle ulteriori finalità di trattamento rispetto a quelle acconsentite inizialmente dall'interessato; titolare che comunque potrà coinvolgere l'Autorità di Controllo qualora ritenga necessaria una adeguata valutazione di impatto. Questa rivoluzionaria *flessibilità valutativa* sulla ricorrenza di ulteriori finalità, risulta la base portante per la l'armonizzazione dei trattamenti di dati personali posti in essere in contesti di forte inferenza informativa, con l'istituto del consenso esplicito e informato e con il principio di finalità.

3. l'introduzione della *privacy by design* e *by default* (cfr considerando 78, art. 25 del Regolamento) insieme alla sicurezza, rappresenta l'innovazione più significativa introdotta dal nuovo Regolamento nella misura in cui – con riferimento alle misure tecniche e organizzative da adottare, prescrivono al titolare le modalità di

[63] Cfr GDPR Art. 6 *Liceità del trattamento,* comma 4)
Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c)della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

progettazione del trattamento, quali mezzi utilizzare (minimizzazione dei dati e pseudonimizzazione) e la fase d'intervento (sin dall'inizio del trattamento stesso).

Il modello *privacy by design/default* sostiene in maniera netta la necessità di minimizzazione dei dati personali oggetto di trattamento come presupposto e misura tecnica preventiva volta ad assicurare all'interessato che il trattamento incroci i principi di qualità dei dati e sia in particolare corretto, lecito, adeguato, pertinente e limitato a quanto necessario rispetto alla prefissata finalità per le quale i dati sono trattati; garantisce quindi il principio di necessità nel corso della progettazione e nella esecuzione del trattamento con riferimento alla quantità dei dati, ai tempi di conservazione e ai livelli di accessibilità;

4. la sicurezza del trattamento e la connessa valutazione dei rischi declinata ai considerando 83, 84 e all'art. 32 del Regolamento[64] è tanto per il titolare che per il responsabile un presupposto concreto vero e proprio per il trattamento, un elemento prioritario e inevitabile che consente al titolare di adempiere alle responsabilità di cui all'art. 24 cioè di assumere e dimostrare di aver assunto ogni misura tecnica e organizzativa adeguata a garantire il rispetto degli obblighi posti dal Regolamento.

   Tra questi obblighi l'art.32 e la dettagliata lista di specifiche in esso contenute, privilegia il dovere per titolare e responsabile del trattamento di mettere in atto *misure tecniche e organizzative adeguare a garantire un livello di sicurezza adeguato al rischio,* facendo riferimento al pari degli art. 24 e 25 alla necessità di tener conto *dello stato dell'arte e dei costi di attuazione, nonché della natura dell'oggetto, del contesto e delle finalità del trattamento.*

   Le misure di sicurezza quindi configurano un quadro regolatorio che pone in capo al titolare e al responsabile di misurarsi fattivamente con la concretezza dei trattamenti e

---

[64] Crf GDPR Sezione 2 *Sicurezza dei dati personali*
Art. 32 *Sicurezza del trattamento*
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. 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.*

dei rischi ad essi connessi;

5. rientra inoltre nell'insieme delle misure di sicurezza dei dati con responsabilità in capo al titolare la valutazione dell'impatto del trattamento dei dati sui diritti e le libertà delle persone interessate (cfr considerando 89-96 art. 35, 36 del Regolamento[65]) ogni qual volta che il trattamento da porre in essere prevede 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.* La valutazione di impatto salvo eccezioni indicate dalla stessa Autorità comporta un dialogo necessario con la stessa Autorità di Controllo (cfr art. 36);

6. l'istituzione del responsabile della protezione dei dati (c.d. *Data Protection Officer,* cfr art. 36-38 del regolamento) obbligatorio nelle Pubbliche Amministrazioni, assolve al ruolo

[65] Cfr GDPR Art. 35 *Valutazione d'impatto sulla protezione dei dati*
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.*
2.I*l titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.*
3.L*a valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:*
a)una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4.L*'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.*
5.L*'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.*
6.*Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.*
7.L*a valutazione contiene almeno:*
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8.*Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.*
9.S*e del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.*
10.*Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.*
11.S*e necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.*

di interfaccia per un collegamento e una cooperazione costante tra il titolare e l'Autorità di Controllo;

7. ulteriore evidenza di questo ricalibrato principio di responsabilizzazione è rappresentata dalle disposizioni relative ai meccanismi certificazione (cfr considerando 77, 81, 100 art. 40 - 43 del Regolamento), che riflettono l'intendimento del legislatore europeo di quanto e come la gestione e la protezione dei dati personali debba assumere parte e rilevanza all'interno dei processi gestionali di enti e aziende;

8. l'introduzione di un Registro delle attività di trattamento[66], in ragione dell'eliminazione dell'adempimento di notifica all'Autorità di Garanzia (Controllo) di particolari trattamenti; è posta in capo al titolare e al responsabile la responsabilità della tenuta dei rispettivi registri che se richiesto dovranno comunque essere resi disponibili alla competente Autorità di Controllo (cfr considerando 82, art. 30 del Regolamento);

9. per quanto attiene invece le violazioni dei dati personali (cfr considerando 85-88, art. 33, 34 del Regolamento, c.d. *data breach*) il titolare del trattamento ha il dovere della

[66] Cfr GDPR Art. 30 *Registri delle attività di trattamento*
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:*
a)il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par. 1.
2.*Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:*
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par 1.
3.*I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.*
4.S*u richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.*
5.*Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di 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.*

notifica alla competente Autorità di Controllo[67] e all'interessato[68] secondo tempistiche e modalità diversificate in relazione alla suscettibilità della gravità delle implicazioni di rischio per i diritti e le libertà delle persone fisiche.

Infine la terza direzione di novità e di sfida - attinente il rafforzamento della cooperazione tra Autorità di Controllo nazionali e tra queste e i titolari del trattamento per il tramite del responsabile della protezione dei dati; un aspetto non secondario e che fa da collante e chiude il cerchio delle questioni poste in essere tanto dai *diritti* tanto dai *doveri,* a cui concorre sia la logica condivisa di un maggior affiatamento e dialogo tra le Autorità sia il rafforzamento dei loro poteri.

Una cooperazione in definitiva volta a incrociare *diritti* e *doveri* affinché la minimizzazione del trattamento sia effettivamente svolta tanto dai soggetti pubblici che privati.

Il maggior dialogo è invocato, in particolare da due novità importantissime alla cui applicazione si rivela essenziale l'intesa, la sinergia e la *governace* delle Autorità di Controllo nazionali:

1. il superamento del criteri di stabilimento con riferimento all'ambito di applicazione

[67] Cfr GDPR Art. 33 *Notifica di una violazione dei dati personali all'autorità di controllo*
1.*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*
2.*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.*
3.La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4.*Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*
5.*Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.*

[68] Cfr GDPR Art. 34 *Comunicazione di una violazione dei dati personali all'interessato*
1.*Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.*
2.*La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).*
3.*Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4.*Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.*

territoriale[69], cfr art. 3 comma 2 lettera b), elemento innovativo anticipato e disceso dagli effetti della sentenza *Google Spain* (2014) con riferimento ai trattamenti posti in essere dai motori di ricerca *on-line*. Nella pratica saranno assoggettati alle Autorità di Controllo tutti i trattamenti svolti sui cittadini europei a prescindere dal fatto che siano effettuati da titolari extra europei o con sedi extra europee a condizione che tali trattamenti attengano l'offerta di beni o di servizi, o il monitoraggio del comportamento nella misura che esso ha luogo all'interno dell'Unione.

La portata di questa innovazione è molto significativa, quasi rivoluzionaria rispetto alla Direttiva (cfr art. 4 *Diritto nazionale applicabile,* e al Codice *privacy* italiano (cfr art. 5 *Oggetto e ambito di applicazione*), rappresentando il presupposto secondo cui – se ne ricorrerà necessità, potranno essere perseguiti grandi colossi come Google Inc., Facebook Inc., Amazon Inc., che non hanno sedi nel territorio dell'Unione.

Ciò intuibilmente implica quanto si riveli basilare un rafforzamento della cooperazione e della *governance* tra le Autorità di nazionali di controllo;

2. l'introduzione del meccanismo dello sportello unico delle imprese (cfr considerando da 123-138 e art. 60-67 del Regolamento, c.d *One Stop Shop*) rappresenta una grossa semplificazione per la gestione dei trattamenti volta a garantirne l'uniformità. Salvo casi specifici le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari paesi dell'Unione per risolvere possibili problematiche connesse all'applicazione e al rispetto del Regolamento potranno rivolgersi ad un solo interlocutore rappresentato dalla locale Autorità di Controllo, sarà poi questa a coinvolgere le altre Autorità di Garanzia.

Al rafforzamento dei poteri delle Autorità di Controllo concorrono:

1. la valutazione dell'impatto dei trattamenti, sulla quale le Autorità di Controllo sono obbligatoriamente chiamate ad esprimersi nel caso in cui dall'utilizzo di nuove tecnologie derivino nuovi rischi per gli interessati oppure per la redazione di linee

[69] Cfr GDPR Art. 3 *Ambito di applicazione territoriale*
1.*Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.*
2.Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.
3.I*l presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.*

guida comprensive anche degli elenchi di trattamenti per i quali la valutazione è imposta o esclusa (cfr considerando da 89 a 96, art. 35 e 36 del Regolamento);

2. la vigilanza sui fenomeni di violazione dei dati personali (c.d. *data breach,* cfr considerando da 85 a 88, art. 33, 34 del Regolamento), atteso l'obbligo in capo al titolare di comunicare eventuali violazioni dei dati all'Autorità di controllo;
3. la figura del responsabile della protezione dei dati quale interfaccia tra l'Autorità di Controllo e il titolare (cfr art. 37- 39 del Regolamento);
4. il rafforzamento dell'aspetto sanzionatorio attraverso criteri comuni e precisi per la valutazione delle violazioni (cfr considerando da 141 a 152, art. 77- 84 del Regolamento).

Infine un importante cambio di prospettiva in coerenza al carattere intrinseco del GDPR di non opporre o rivelarsi ostativo della libera circolazione e del libero scambio di informazioni in una società inevitabilmente interconnessa oltre ogni confine, è quello del trasferimento dei dati verso paesi terzi o organizzazioni internazionali.

Questa parte è contenuta al capo V - *Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali,* risultante dagli art. 44-50 e che per lo spessore e le argomentazioni può essere considerato un sotto regolamento al GDPR.

4. IL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (UE) 2016/679: *IL SOGGETTO INTERESSATO E IL DATO PERSONALE.*

L'implementazione del diritto alla protezione dei dati personali come controllo sugli stessi è uno dei punti cardine del nuovo Regolamento Europeo 679 del 2016.

Ad evidenziarne l'importanza si richiama la premessa indicata al considerando 7): è *opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche;* e quella del considerando 85): *Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.* <...>[70] - quest'ultimo risulta significativo per considerare la perdita di controllo sulle proprie informazioni al pari di altre violazioni e di altri utilizzi illeciti (furto, impersonazione, perdita di diritti, discriminazione, lesione della reputazione....).

Il Regolamento eredita dalla Direttiva madre la caratteristica di attuare la protezione dei dati personali come controllo sugli stessi, mantenendo e rafforzandone in maniera stringente il paradigma regolatorio del trattamento [*informativa-finalità-consenso*] al centro del quale il soggetto interessato si pone per il tramite di tutta una serie di diritti da questi azionabili.

Il consenso[71] rientra tra le basi legali del trattamento – oltre all'esecuzione di un

---

[70] <segue dal considerando> *Pertanto, non appena viene a conoscenza di un avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*

[71] Cfr GDPR considerando 32) (32) Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.
Art. 4 *Definizioni*
comma 11) Consenso: «consenso dell'interessato»:qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Articolo 6 *Liceità del trattamento*
1.Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

contratto, la ricorrenza di un obbligo legale, salvaguardia di superiori e vitali interessi, interesse pubblico, legittimo interesse, ulteriori finalità valutate compatibili a quelle iniziali (e acconsentite dalla persona interessata); concorre a configurarne la liceità e l'autorizzazione; espone la dichiarazione di volontà del soggetto interessato, positiva e inequivocabile: rappresenta la prima (informata) azione di controllo dei soggetti interessati contingente al rilascio (*disclosure*) dei propri dati personali.

Come anticipato nel precedente paragrafo (sulle principali novità introdotte dal Regolamento europeo) il GDPR introduce una disciplina del consenso informato ed esplicito molto più stringente rispetto alla Direttiva[72] in cui la *generalità* (cfr art. 4 *Definizioni* comma 11): *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato* <...>) viene compensata e contenuta con/dalla *inequivocabilità;* e la (formale) accettazione prevista nella definizione della Direttiva madre superata ed estesa dall'azione positiva, fattiva e concludente del soggetto interessato (cfr art. 4 *Definizioni* comma 11): <...> *mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*).

Le proprietà che indicano e misurano la *qualità* del consenso qualificandolo in termini di robustezza, validità (rispetto alla liceità del trattamento) ed efficacia (rispetto alla valorizzazione e al mantenimento nel tempo degli effetti delle sue caratteristiche), possono essere così rappresentate: *i)* consenso *necessario:* il consenso è necessario per legittimare il trattamento dei dati personali – in assenza di ulteriori previsioni legislative specifiche che autorizzano il trattamento; *ii)* consenso *informato:* il consenso deve essere informato, ovvero preceduto da valida e idonea informativa, nella quale in particolare la natura del trattamento sottoposto a consenso dovrebbe essere spiegata in forma intellegibile, facilmente accessibile, in forma semplice, chiara e non ambigua e priva di clausole abusive; *iii)* consenso *libero:* il consenso deve rappresentare la scelta vera, libera, consapevole e priva di condizionamenti

<...>
Articolo 7 *Condizioni per il consenso*
1.Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2.Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3.L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4.Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

[72] Cfr DIRETTIVA art. 2 Definizioni lettera h) «consenso della persona interessata»: qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento.

dell'interessato; questo requisito è strettamente legato per un verso alla correttezza e esaustività dell'informativa e per un altro misurato in rapporto alle implicazioni che deriverebbero in caso di diniego dell'interessato al rilascio delle informazioni personali; *iv)* consenso *specifico:* il consenso segue la finalità e, in casi di ulteriori finalità, deve essere prestato distintamente per ciascuna di esse anche per lo stesso trattamento; il consenso deve riferirsi ad un contesto ben individuato e specifico di trattamenti, calibrato alle necessità del soggetto interessato; *v)* consenso *evidente:* il consenso – può essere espresso tramite una dichiarazione o l'evidenza di una azione positiva e concludente del soggetto interessato, comunque attraverso qualsiasi modalità che consenta di esprimere ed esporre una volontà informata, libera e specifica – in uno specifico contesto, ad accettare il trattamento.

Infine: il consenso può essere revocato dall'interessato in qualsiasi momento, e di tale facoltà e di tale diritto l'interessato deve essere informato prima del rilascio; il Regolamento pone l'onere della prova del consenso in capo al titolare del trattamento.

Se il consenso rappresenta la prima (informata) azione del controllo dei soggetti interessati, il mantenimento di tale controllo è effettuato per il tramite di ben definiti diritti azionabili dal soggetto interessato, diritti che il titolare e il responsabile sono tenuti a conoscere non solo per riscontrare eventuali richieste prodotte dalla persona interessata ma anche per essere in condizione di configurare correttamente e sin dalla progettazione del trattamento (cfr art. 25 - *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita tutte le misure di carattere tecnico, organizzativo, di sicurezza)* tutte le misure tecniche, organizzative e di sicurezza – e tra queste ultime, in particolare, la valutazione dell'impatto del trattamento e dei rischi; cfr art. 32 - *Sicurezza del trattamento*, 35 - *Valutazione d'impatto sulla protezione dei dati*); nonché per valutare l'occorrenza di eventuali violazioni e adempire alle conseguenti notifiche (cfr art. 33 - *Notifica di una violazione dei dati personali all'autorità di controllo;* e art. 34 - *Comunicazione di una violazione dei dati personali all'interessato).*

I diritti azionabili dall'interessato si suddividono in diritti di natura conoscitiva e in diritti regolanti il controllo vero e proprio dei dati personali. Alla prima categoria appartengono:

1. Il Diritto all'informativa (cfr considerando 58, 60; art. 13 *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato* e art. 14 *Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato)* stabilisce che l'interessato ha diritto ad essere informato mediante apposita informativa che per essere idonea deve esporre con chiarezza e senza ambiguità specifici contenuti in merito l'esistenza del

trattamento, le sue finalità - anche ulteriori, l'identità del titolare, l'occorrenza di una profilazione e le relative implicazioni, i diritti azionabili sul trattamento e le relative modalità di esercizio – in particolare la revoca del consenso e compreso il diritto alla portabilità, la ricorrenza del legittimo interesse quale caratteristica del trattamento, l'eventuale trasferimento dei dati al di fuori dell'Unione e con quali garanzie; nel caso i dati siano raccolti presso la persona interessata l'informativa deve essere esposta al momento della raccolta, diversamente se raccolti presso altre fonti la tempistica dovrebbe essere definita in coerenza alle circostanze.

Il Regolamento stabilisce un'eccezione generale all'informativa: la non necessarietà dell'obbligo se l'interessato dispone già dell'informazione, se le operazioni di trattamento sono previste per legge, se informare l'interessato si rivela impossibile o richiede uno sforzo sproporzionato quando per esempio nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica, o a fini statistici.

L'informativa è un adempimento che rimane a carico sia di soggetti pubblici e privati, ricalca sostanzialmente quanto previsto dal Codice *privacy* italiano, in particolare in ordine alla descrizione del legittimo interesse, in alcuni casi da solo sufficiente a fondare la liceità del trattamento.

L'informativa diventa sempre maggiormente presupposto e strumento di trasparenza riguardo il trattamento e l'esercizio dei diritti. Per facilitare la comprensione dei contenuti nell'informativa si potrà fare riferimento anche ad icone identiche in tutta l'Unione Europea. L'informativa è inoltre condizione necessaria e sufficiente del consenso.

2. Il Diritto all'accesso (cfr considerando 63; art. 15[73] *Diritto di accesso dell'interessato):*

[73] Cfr GDPR art. 15 *Diritto di accesso dell'interessato*

1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a)le finalità del trattamento;

b)le categorie di dati personali in questione;

c)i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e)l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f)il diritto di proporre reclamo a un'autorità di controllo;

g)qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h)l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. *Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.*

3. *Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta*

all'interessato è garantito il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente ad intervalli di tempo ragionevoli per essere consapevole del trattamento e verificarne periodicamente la liceità. Tale diritto consiste nel conoscere e ottenere comunicazioni con particolare riguardo alle finalità e alle modalità di trattamento. Il titolare è tenuto a verificare l'identità dell'interessato richiedente in particolare se le richieste sono prodotte *on-line,* e a riscontrare la richiesta di accesso fornendo una copia di dati o consentendo all'interessato un accesso remoto ai dati per la consultazione.

Alla seconda categoria, quella del controllo sui dati, appartengono:

1. Il Diritto alla rettifica e all'integrazione (cfr considerando 39, 59, 65, 73; art. 5 comma 1) lettera d); art. 16[74]). L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei propri dati personali inesatti senza ingiustificato ritardo.

   In relazione alle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

   Il titolare è tenuto anche a comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o comporti uno sforzo sproporzionato.

   Tale diritto oltre ad essere uno strumento di controllo è anche uno strumento mantenimento della qualità dei dati in attinenza al requisito dell'*esattezza*[75].

2. Il Diritto alla cancellazione e all'oblio (cfr considerando 65, 66, 68; art. 17[76] *Diritto alla*

mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
4. *Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.*

74 Cfr GDPR Art. 16 *Diritto di rettifica*
L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

75 Cfr GDPR, Art. 5 *Principi applicabili al trattamento di dati personali*
1. *I dati personali sono:*
<...>
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»);

76 Cfr GDPR Art. 17 *Diritto alla cancellazione («diritto all'oblio»)*
1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:*
a)i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b)l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c)l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d)i dati personali sono stati trattati illecitamente;
e)i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

cancellazione («diritto all'oblio»)): l'interessato ha il diritto di ottenere dal titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare ha l'obbligo di riscontrare la richiesta, se sussistono determinate ragioni: ad esempio ritenuti non più necessari o trattati in maniera non lecita, in caso di revoca del consenso o di opposizione dell'interessato al trattamento.

3. Il Diritto alla limitazione (cfr considerando 67; art. 18[77] *Diritto di limitazione di trattamento)*: l'interessato ha il diritto – se ricorrono determinate motivazioni, di chiedere una limitazione del trattamento, intesa come restrizione ad alcune operazioni di trattamento, ad esempio limitandolo alla sola conservazione. Alcune delle motivazioni possono concernere l'esattezza dei dati trattati dal titolare, oppure operazioni ritenute illecite; la limitazione può anche opporre la cancellazione ponendo dei vincoli all'utilizzo oppure intervenire nelle more che sia riscontrata una richiesta all'esercizio del diritto di opposizione prodotta dalla persona interessata.

4. Il Diritto all'opposizione (cfr considerando 50, 59, 69, 70, 73; art. 21[78] *Diritto*

f)i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. *Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.*

3. *I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:*

a)per l'esercizio del diritto alla libertà di espressione e di informazione;

b)per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c)per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d)a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e)per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

[77] Cfr GDPR Art. 18 *Diritto di limitazione di trattamento*

1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:*

a)l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b)il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c)benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d)l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. *Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.*

3. *L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.*

[78] Cfr GDPR Art. 21 *Diritto di opposizione*

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

all'opposizione): l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

Il titolare del trattamento è tenuto ad astenesi dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. L'interessato può esercitare tale diritto anche contro trattamenti di profilazione – connessi al *processo decisionale automatizzato relativo alle persone fisiche*[79].

5. Il Diritto alla portabilità dei dati (cfr considerando 68, 73; art. 13 *Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato* e art. 20[80] *Diritto alla portabilità dei dati*). Il diritto alla portabilità è uno dei (nuovi) diritti introdotti dal Regolamento di maggior portata pratica, completa il diritto di accesso, sostiene la qualità del dato

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.
4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

[79] Cfr GDPR Art. 22 *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*
1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
2. *Il paragrafo 1 non si applica nel caso in cui la decisione:*
a)sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
b)sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c)si basi sul consenso esplicito dell'interessato.
3. *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*
4. *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.*

[80] Cfr GDPR Art. 20 *Diritto alla portabilità dei dati*
1. L*'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:*
a)il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
b)il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

indirizzandone una standardizzazione e una interoperabilità del formato, e in definitiva rafforza l'azione di controllo da parte della persona interessata esercitabile sui propri dati quando questi sono trattati con strumenti automatizzati.

Questo diritto stabilisce che l'interessato deve poter ricevere dal titolare del trattamento tutti i dati personali che lo riguardano in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile, in modo da poterli all'occorrenza trasmettere agevolmente ad un altro titolare del trattamento.

Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati.

Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto non dovrebbero segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura e per il tempo in cui i dati personali sono a tal fine necessari.

5. QUESTIONI APERTE.

I principali punti aperti rintracciati nel periodo di tempo successivo all'approvazione del Regolamento (UE) 2016/679 possono essere riconducibili al passaggio dalla Direttiva 95/46/CE al Regolamento, alle modalità e alla tempistica di attuazione di quest'ultimo, al cambiamento di impostazione e di prospettiva.

Il Regolamento (UE) 2016/679 è stato pubblicato nella Gazzetta Ufficiale dell'Unione del 4 Maggio 2016, entrato in vigore il 25 Maggio dello stesso anno trovando però attuazione solo dal 25 Maggio 2018 data a decorrere dalla quale verranno abrogata la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 e le leggi nazionali.

La tempistica di attuazione del Regolamento pone da oggi e sino al 24 Maggio 2018 un ambito di criticità legato al differimento dell'efficacia, differimento peraltro parziale e all'interno del quale si possono distinguere:

1. un non banale problema di compresenza di due normative profondamente diverse nella forma, nell'impostazione, nella prospettiva – la prima *nazionale/individuale,* la seconda *europea/relazionale* – che nel periodo di transizione comportano la messa in atto di tutta una serie di adempimenti nonché e soprattutto di un cambio di mentalità e di approccio verso la protezione dei dati personali dall'adempimento *formale* alla responsabilità *sostanziale*;

2. la complessità di tali adempimenti che per un verso rassicurano sulla continuità dell'efficacia delle decisioni assunte vigendo la Direttiva e per un altro invocano la conformità al GDPR[81].

   Per molte parti, infatti, il GDPR è immediatamente vincolante laddove, ad esempio, indica che le attività di trattamento già in corso - ed in particolare il consenso, effettuate ai sensi della Direttiva devono essere rese conformi al Regolamento entro i due anni che ne precedono l'attuazione e la contestuale abrogazione della Direttiva; al contempo, tuttavia, l'art. 94 del GDPR - *Abrogazione della direttiva 95/46/CE* rassicura che i riferimenti alla Direttiva abrogata si intendono trasposti al Regolamento, e che (considerando 171) l'attuazione del GDPR al 25 Maggio 2018 non comporterà la la

[81] Cfr GDPR considerando 171) Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.

perdita di efficacia degli atti e delle decisioni assunte dalle Autorità Nazionali ai sensi delle leggi nazionali e vigendo la Direttiva.

Il processo di transizione, inoltre, investe più attori: *i)* gli Stati chiamati a modificare la legislazione sull'Autorità di controllo locali e a valutare cosa trattenere delle leggi nazionali vigenti e cosa abrogare; *ii)* la Commissione chiamata modificare il Regolamento 2001/45 *concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati* e la Direttiva *e-privacy* 2002/58/EC sulle comunicazioni elettroniche per renderli conformi al GDPR; ma *iii)* soprattutto i titolari del trattamento, nella misura in cui devono rendere conformi al Regolamento i trattamenti già in corso in un contesto in cui quest'ultimo non è attuato e la Direttiva - nonché le leggi di attuazioni nazionali, sono ancora in vigore e pienamente efficaci richiedendo il necessario rispetto;

3. un eccesso flessibilità del Regolamento che solo in parte si rivela uno strumento giuridico garanzia di uniformità e coesione. Le parti in cui, infatti, il Regolamento intreccia la normativa nazionale consentendo alle leggi nazionali di poter integrare, attuare, derogare e sostituire non sono ne poche ne tali da essere trascurate per lo spessore delle argomentazioni trattate. Gli ambiti che rimangono di competenza dei singoli Stati pur in coerenza e in rispetto ai principi generali del Regolamento, sono quelli indicati al Capo IX *Disposizioni relative a specifiche situazioni di trattamento*[82]; gli Stati membri possono intervenire interstizialmente sul regolamento (quindi modificarne le norme) con riguardo all'introdurre ulteriori limitazioni rispetto a quelle già previste per il trattamento di dati genetici, dati biometrici o dati relativi alla salute che siano raccolti con il consenso dell'interessato ma utilizzati anche per finalità diverse rispetto a quelle iniziali[83]; per stabilire l'età compresa tra i 13 (limite minimo fissato dal GDPR) e i 16 anni in caso di consenso prestato dal genitore del minore[84]; oppure intervenire sulle

[82] Art. 85 *Trattamento e libertà d'espressione e di informazione*
Art. 86 *Trattamento e accesso del pubblico ai documenti ufficiali*
Art. 87 *Trattamento del numero di identificazione nazionale*
Art. 88 *Trattamento dei dati nell'ambito dei rapporti di lavoro*
Art. 89 *Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*
Art. 90 *Obblighi di segretezza*
Art. 91 *Norme di protezione dei dati vigenti presso chiese e associazioni religiose*

[83] Cfr GDPR Art. 9 *Trattamento di categorie particolari di dati personali* <...>
comma 4) Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.
Considerando 53) <...> *Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.*

[84] Cfr GDPR Art. 8 *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione,*
comma 1) Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società

norme sanzionatorie prevedendone nuove fattispecie oppure fissare il limite minimo della misura (rispetto a quello massimo fissato dal GDPR); gli Stati membri potranno intervenire sulla regolamentazione della *Privacy by Design/Default,* nella definizione degli indicatori per la valutazione dell'impatto del trattamento e nella definizione delle misure di sicurezza; agli Stati membri è infine attribuito il potere derogatorio sui processi decisionali automatizzati e di profilazione[85] effettuati senza il consenso esplicito dell'interessato; sui trattamenti esplicitamente soggetti a limitazione (art. 23 *Limitazioni*, per tutta la parte attinente la sicurezza nazionale che esula dall'essere ricoperta dalla normativa sulla protezione dei dati personali).

Quanto precede indica come in realtà sia flessibile il Regolamento e quanto permanga sostanziale e complesso l'intreccio con la legislazione dei singoli Stati membri rispetto al quale solo una fattiva cooperazione delle Autorità di Controllo potrà evitare far *retrocedere* il Regolamento ad una sorta di Direttiva di armonizzazione.

Agli ambiti premessi si aggiunge un punto aperto legato alla più importante caratterizzazione del GDPR e la cui portata andrà ben oltre il biennio di adozione:

4. la prerogativa nativa del GDPR a non voler assolutizzare il diritto alla protezione dei dati personali introduce (tra l'altro) un accrescimento e un ripensamento della responsabilità del titolare[86] per un verso, e dei poteri delle Autorità di Controllo e del Comitato Europeo per un altro, ai quali purtroppo non è seguita una compensazione in termini di valorizzazione della responsabilità del soggetto interessato: alla positivizzazione dell'*accontability* non è stata affiancata una positivizzazione dell'*empowerment* del soggetto interessato.

   Azione, questa, che si sarebbe rivelata strumentale non solo a rafforzare il controllo dei propri dati e il principio di autodeterminazione informativa (elementi questi

dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.
Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni. 4.5.2016 L 119/37 Gazzetta ufficiale dell'Unione europea IT.

85 Cfr GDPR Art. 22 P*rocesso decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*
1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

86 In tal senso si richiama, rispetto a quanto già illustrato nel precedente paragrafo 3, che la positivizzazione del principio di *accountabilty* comporta per il responsabile una assunzione di responsabilità che non si esaurisce all'adempiere ad una norma giuridica divenendo una vera e proprio assunzione di rischio.

indubbiamente mantenuti e ampiamente consolidati nel Regolamento) ma anche ad instaurare un meccanismo virtuoso - con al centro il soggetto interessato, volto ad attuare una sorta di appropriazione delle proprie informazioni personali oggetto e derivanti dal trattamento, e soprattutto un accrescimento della consapevolezza dell'importanza e del valore dei propri dati personali.

Il passaggio dalla Direttiva madre al GDPR potrebbe comportare - per le riflessioni che ad oggi si sono potute sviluppare, se non una limitazione sicuramente un mancato accrescimento della centralità dell'utente in ragione del prevalere di quella del titolare e del responsabile al trattamento.

Questa valutazione trova supporto e riscontro in tre elementi del Regolamento:

i. nonostante il Regolamento abbia consolidato il diritto alla protezione dei dati personali come diritto di controllo sugli stessi e posto in essere tramite l'autodeterminazione del soggetto interessato, e nonostante il Regolamento abbia formalizzato un vero e proprio istituto del consenso rendendolo più stringente, non sono seguiti efficaci e nuovi meccanismi di mantenimento dei requisiti di qualità ne interventi sui diritti di controllo azionabili dall'interessato essendo rimasti sostanzialmente invariati rispetto alla Direttiva (fatta eccezione per l'introduzione del diritto alla cancellazione, all'oblio e alla portabilità);
ii. tra le varie responsabilità il GDPR pone in capo al titolare quella di poter valutare la compatibilità delle finalità laddove (in assenza di consenso o ad autorizzazione non ancora rilasciata) il trattamento ne introduca diverse da quella iniziale; il positivo incrocio di tale compatibilità sulla base dei requisiti esposti dall'art. 6 - *Liceità del trattamento*, comma 4[87], se per un verso rappresenta una determinazione di flessibilità nella gestione del trattamento per un altro pone in subordine il soggetto interessato nel valutare, nell'essere pienamente consapevole e quindi nell'autorizzare utilizzi e scopi secondari.
iii. i meccanismi di notifica delle violazioni, di fatto, subordinano la comunicazione al

[87] Articolo 6 - Liceità del trattamento, comma 4
Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:
a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
c)della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione

soggetto interessato ad un doppio passaggio valutativo: quello del titolare e quello dell'Autorità di Controllo, sui quali è posta la responsabilità di valutare se e come una avvenuta violazione abbia ricadute dirette e misurabili, in termini di gravità, sui diritti e le libertà delle persone.

Appare singolare infatti che di fronte – ad esempio, ad una perdita di dati personali il titolare non abbia il dovere – in linea di principio, di comunicarlo prioritariamente e con precedenza al soggetto interessato; anzi che non sia tenuto a farlo se risulta improbabile che la violazione dei dati personali presenti rischi per la persona.

Il diritto dell'interessato a conoscere risulta residuale, secondario. La comunicazione all'interessato è infatti – per quanto disposto dagli art. 33 e 34, subordinata all'esito della valutazione della ricorrenza della gravità di rischio per la tutela dei diritti e delle libertà dell'interessato associabile al trattamento, valutazione effettuata dal titolare e dall'Autorità di Controllo.

La ragione per la quale vengono così caricate tanto la responsabilità del titolare, tanto quella delle Autorità di Controllo e il potere di queste, probabilmente discende dalla volontà di base del legislatore europeo a non voler assolutizzare il diritto alla protezione dei dati personali perché si mantenga non ostativo alla funzione sociale e allo scambio delle informazioni.

CAPITOLO 2

PRIVACY E PROTEZIONE DEI DATI PERSONALI: PLURALITÀ SEMANTICHE E CRITICITÀ

SOMMARIO: 1. I dati e le informazioni personali. – **1.1.** Le proprietà del dato personale, la gestione e gli attori coinvolti. – **1.2.** La centralità dell'utente nel *disclosure* dei dati personali. **– 1.3**. Ripensare il concetto di dato personale. – **1.4.** La modellazione dei Dati Personali. – **2.** La *Privacy* e la protezione dei dati personali. – **2.1.** I molteplici significati della *Privacy.* – **2.2.** La modellazione della *Privacy.* – **2.3** Protezione dei dati personali: le criticità e rischi connessi alla gestione del dato. **– 2.4.** Protezione dei dati personali: la centralità dell'utente tra *status quo,* trasparenza e controllo.

1. I DATI E LE INFORMAZIONI PERSONALI.

I sistemi di gestione delle informazioni digitali in poco più di mezzo secolo - a partire dagli anni '60, si sono evoluti da sistemi di calcolo numerico in ambito scientifico e militare (centralizzati e prerogativa di pochi e potenti centri di calcolo) a sistemi di registrazione, elaborazione e riproduzione dei dati economici e sociali - che, grazie allo sviluppo congiunto delle tecniche di memorizzazione a basso costo e delle banche dati - pur mantenendo una configurazione centralizzata, potevano essere archiviati, collegati e integrati in misura sempre maggiore; per diventare – oggi, sistemi di gestione e di produzione della conoscenza.

La diffusione dei personal computer in ogni ambito della vita sociale, ma in particolare la connessione di questi in rete e successivamente tramite Internet, attua un cambiamento radicale tanto da trasformare le architetture da centralizzate a distribuite, le applicazioni e il *workflow* da *mainframe* a *client/server* ma soprattutto tale da modificare totalmente il canale di produzione e di rilascio delle informazioni coinvolgendo l'utente come principale produttore e latore virtuale dei propri dati personali: un passaggio epocale che qualifica i *dati* (personali) *contenuti in ogni singolo computer come frammenti dell'immenso deposito di informazione della rete stessa,* (potenzialmente) *accessibili* (in entrata e in uscita) *da ogni utente della rete e collegabili con ogni altra informazione - indipendentemente dalla collocazione geografica*[88], tramite servizi prima inesistenti o erogati ad un costo monetario significativo nelle equivalenti forme del mondo reale (si pensi alla posta elettronica, alle ricerche sui motori di ricerca, ai servizi di networking in genere).

[88] Sartor G., *Il Diritto alla protezione dei dati personali*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, Prefazione p. XIII-XVI.

Il resto della storia - che evolve il *personal computer* in *device* ed affianca all'utente gli *oggetti,* è segnato dal *wireless* e dal *mobile,* dalle *disruptive technlogies* e, tra queste, in particolare il *Cloud computing* e l'*IoT*[89], che interconnesse e alimentate dai *Social Network* proiettano la persona in un ambiente totalmente informazionale. Ma non secondariamente anche dalle (nuove) tecniche per la strutturazione e la rappresentazione delle informazioni: le etichettature semantiche, i meta-linguaggi, il Web semantico – domini del *data mining* e degli algoritmi statistici di inferenza, rendono possibile l'estrazione di informazioni e del loro significato da insiemi di dati sempre più voluminosi, vari e differenziati, veloci nel generarsi (*Big Data*), puntando a rendere tale significato non solo *machine-readable* ma anche *machine-understandable.*

In definitiva un complesso di architetture, applicazioni e algoritmi che - con al centro la persona, nel tempo, hanno consacrato i sistemi di gestione delle informazioni come sistemi produttori, divulgatori e manipolatori di conoscenza; hanno catalizzato lo sviluppo e l'affermarsi di nuove tecnologie di miglioramento ma anche di intrusione nella sfera individuale; al contempo – in parallelo, hanno indirizzato e diversificato il significato e le caratteristiche della *privacy* e della protezione dei dati personali (cfr successivo paragrafo 2. - *La Privacy e la protezione dei dati personali*).

Datification, Data Revolution e *Data-accretion* sarebbe l'espressione più attuale e corretta. La rivoluzione del *Big Data*, già etichettato come il capitalismo dei dati[90], evolve a ritmi

[89] L'affermazione del *Cloud Computing* e l'*Internet of Things* - rispettivamente intesi come l'infrastruttura che eroga *on demand* risorse informatiche e servizi informatici (archiviazione, elaborazione, trasmissione); e come l'insieme degli oggetti sempre più interconnessi capaci di inviare e ricevere informazioni, si sovrappone e fa seguito agli effetti della contestuale stabilizzazione della prima legge di Moore che, rallentando, si accinge a raggiungere la fine del suo percorso (Fonte Economist, Intel Inc. 2016). Il ciclo di raddoppio dei componenti e delle performance computazionali, a parità di costo, si è rimodulato a quadruplo e, prevedibilmente, non sarà soggetto di ulteriori estensioni per i limiti imposti dalla stessa fisica e connessi all'impossibilità di miniaturizzare all'infinito i minuscoli transistor dei circuiti integrati. Ciò ha indirizzato e favorito un cambiamento nei sistemi architetturali: la potenza di calcolo del *cloud computer* - risultante di numerosi server connessi in parallelo, ha reso sempre meno necessaria la presenza di processori potenti sui personal computer, i quali (quindi) tendono ad essere sostituiti da *devices* capaci di interconnettersi rapidamente in banda larga. Ma ciò che si eredita dalla stabilizzazione della prima legge di Moore non è solo il limite computazionale componenti/performance bensì l'estrema minimizzazione del costo della potenza di calcolo, presupposto della pervasiva diffusione dell'*IoT*: il costo di un tag RFID è talmente irrisorio (mediamente 0,10 Euro) da registrare una produzione di 13 trillion di transistor per secondo, e nella pratica di consentirne il posizionamento in qualunque tipo di oggetto della vita quotidiana, al punto da stimare per l'anno 2020 la presenza di 50 miliardi di devices contro la previsione di 8 miliardi di persone. In argomento si rimanda alla consultazione delle seguenti fonti:
http://www.economist.com/technology-quarterly/2016-03-12/after-moores-law (12 Marzo 2016)
Atti seminario Prof. Luciano Floridi, su *Internet of Things* per i 30 anni di Internet in Italia.
Presso CIRSFID, Università di Bologna (30 Aprile 2016)
http://www.anandtech.com/show/10959/intel-launches-7th-generation-kaby-lake-i7-7700k-i5-7600k-i3-7350k (3 Gennaio 2017)
http://www.lastampa.it/2017/02/13/tecnologia/news/addio-legge-di-moore-i-chip-dei-computer-non-corrono-pi-come-una-volta-TSPv1TZAjuq7iy4t13bM5K/pagina.html (13 Febbraio 2017)

[90] In argomento la fonte è consultabile su: *Capitalismo digitale, ecco le nuove sfide* di Anotonio Nicita e Antonio Preto – che tra l'altro illustra come nuove forme di prorietà privata digitale siano connesse alla libertà di espressione di Internet che implicitamente alimenta il volume di dati prodotto, utilizzato o sfruttato da altri. http://www.ilsole24ore.com/art/commenti-e-idee/2014-10-27/capitalismo-digitale-ecco-nuove-sfide--084012.shtml?uuid=ABKYA96B&refresh_ce=1 (27 Ottobre 2014)

velocissimi. Comunicazioni, tecnologie e dinamiche economiche si basano sempre più sul continuo e massivo scambio di dati tramite Internet[91], veicolato dalle *Internet disruptive technologies,* e distinto da un elevatissimo potenziale di inferenza e deduzione. Sull'argomento, con specifico riferimento al *Cloud Computing* e all'*IoT,* si ritiene significativo riportare alcune proiezioni quantitative intercettate da fonti autorevoli del settore, con la finalità di rappresentare l'impatto della forte crescita *in quantità* delle informazioni digitali dalla quale si muove e dipende anche una crescita *in qualità,* ogniqualvolta diventa possibile interpretare e analizzare la quantità di dati raccolti per definire un'associazione (diretta o indiretta) di attribuzione e di indentificabilità con le persone, ovvero quando i *dati* (di rete, di dispositivi, di sistema o applicativi) diventano (se già non lo sono perché rilasciati, disposti o richiesti volontariamente degli utenti) *dati personali,* sempre più soggetti a utilizzi secondari e ulteriori difficilmente prevedibili.

Gartner Inc.[92] stima che ogni giorno del 2016 ha contato 5,5 miliardi di dispositivi interconnessi, per prevederne il triplo (20,8 miliardi) nel 2020[93]. Stima confermata da **Cisco System Inc.**, nell'ambito dell'iniziativa *Cisco Visual Networking Index (VNI)* volta a tracciare e prevedere negli anni lo sviluppo e l'impatto delle applicazioni di networking (Figura 2.1).

Ibm documenta che nel mondo vengono già generati 2,5 quintilioni di byte (10^{30} byte) di dati ogni giorno: il 90% di tutti i dati nel mondo è stato creato negli ultimi due anni[94]. Secondo la previsione di **Cisco System Inc.** (contenuta nella sesta edizione del suo *Global Cloud Index* 2015-2020, report che mappa il settore e fornisce indicatori dei vari trend in atto) il traffico cloud aumenterà di quasi 4 volte fra il 2015 e il 2020, passando da 3,9 a 14,1 zettabyte[95] l'anno, data entro la quale il 92% dei *workload* verrà processato da *data center* cloud, e

---

Svolta "datification": così i big data fanno cassa sulla privacy di Patrizia Licata, Nel capitalismo dei dati la privacy non è necessariamente distrutta, dicono gli esperti: ridando agli utenti il controllo sulle info si realizzerà un mondo più smart, senza rinunciare ai diritti fondamentali.
http://www.corrierecomunicazioni.it/it-world/45271_svolta-datification-cosi-i-big-data-fanno-cassa-sulla-privacy.htm

91 In argomento appare significativo riportare il dato che Cisco System Inc., nell'ambito dell'iniziativa *Cisco Visual Networking Index (VNI)*, pubblica in merito all'andamento storico del traffico Internet, passato da 100 GB al giorno nell'anno 1992, a 100 GB per ora nel 1997, a 100 GB per secondo nel 2002, che diventano 2000 nell'anno 2007 e 20,235 nel 2005. Per infine stimare 61.386 GB per secondo nel 2020
cfr *Zettabyte Era — Trends and Analysis – Cisco*
http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html
(02 Giugno 2016)

92 Gartner Inc. è una multinazionale leader mondiale nella consulenza strategica, ricerca e analisi nel campo dell'Information Technology .

93 In argomento la fonte è consultabile su: *Gartner prevede 20 miliardi di oggetti IoT connessi nel 2020.*
http://www.silicon.it/networks/gartner-prevede-20-miliardi-di-oggetti-iot-connessi-nel-2020-88394 (11 Novembre 2015)

94 In argomento la fonte è consultabile su: *Con TECHNOGYM e IBM, l'intelligenza artificiale nel wellness,* di Paola Piacentini e Alessandro Ferrari. http://www-03.ibm.com/press/it/it/pressrelease/51780.wss (08 Marzo 2017)

95 1 zettabyte = 10^{21} byte

solo il residuale 8% *data center* tradizionali[96] (Figura 2.2).

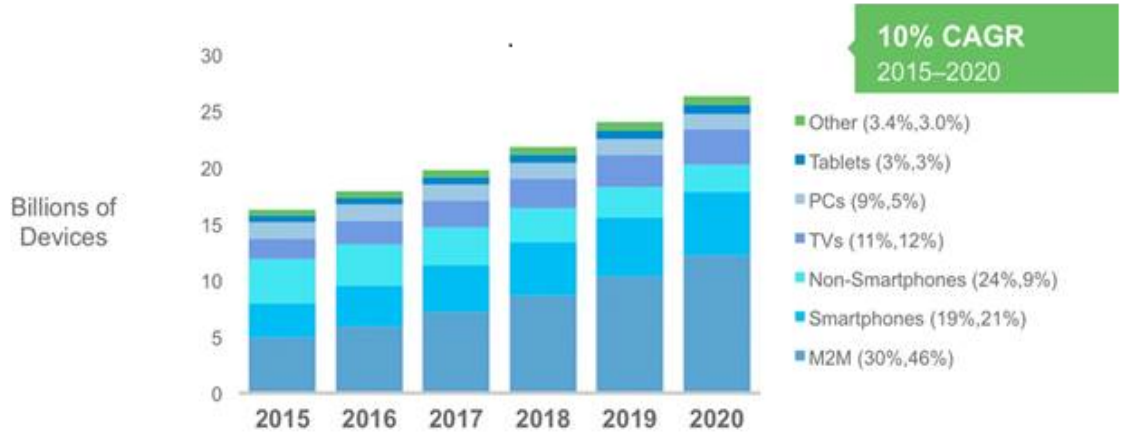


Figura 2.1 – Andamento di crescita tra il 2015 e il 2010 del numero di devices e connessioni (fonte CISCO System Inc.[97])

Il grafico evidenzia che - sulla base della comparazione CAGR (Compound Annual Growth Rate), la crescita di devices e connessioni (10% CAGR) è più veloce sia della crescita della popolazione (stimata al 1% CAGR) che degli utenti Internet (stimata al 6% CAGR)

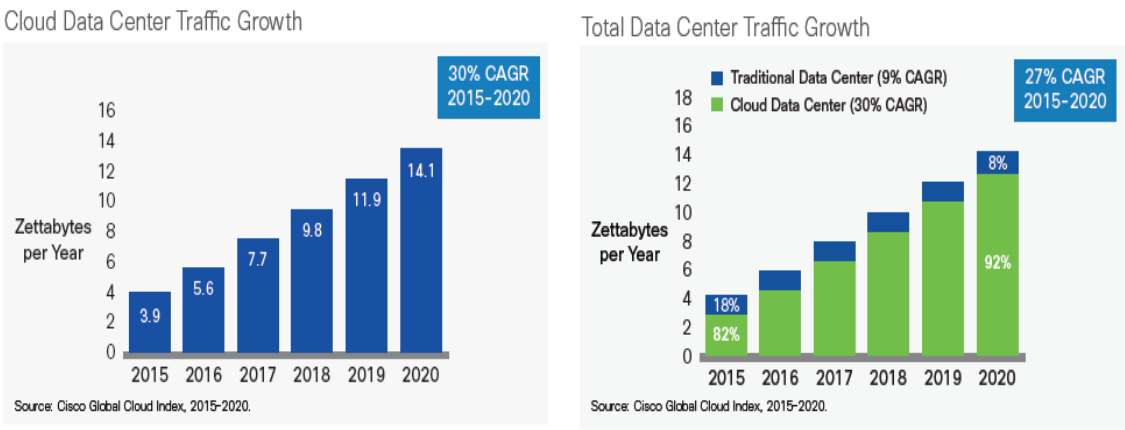


Figura 2.2 – Comparazione e andamento di crescita del traffico *Cloud* nel periodo 2015-2020 (Fonte Cisco System Inc.)

[96] In argomento la fonte è consultabile su: *The Zettabyte Era — Trends and Analysis – Cisco* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html (02 Giugno 2016)
White Paper Cisco Global Cloud Index: Forecast and Methodology, 2015–2020 http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf
Ed inoltre su: *Cloud, boom in arrivo: nel 2020 viaggeranno 14,1 zettabyte di dati*, di Andrea Frollà. http://www.corrierecomunicazioni.it/digital/44489_cloud-boom-in-arrivo-nel-2020-viaggeranno-141-zettabyte-di-dati.htm (16 Novembre 2016)

[97] *The Zettabyte Era — Trends and Analysis – Cisco* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html (02 Giugno 2016)

L'interpretazione significativa di queste proiezioni quantitative riguarda il sottoinsieme dei dati estraibili, relativi a servizi o applicazioni (di *business* o *personal)* connesse ad azioni concrete degli utenti: in cui l'utente assume un ruolo centrale, in cui l'informazione digitale connessa ad un nome o ad informazione identificativa diventa dato personale.

Gli esempi attengono tutti gli aspetti della vita quotidiana: il commercio, la finanza, le assicurazioni, i trasporti, l'energia, la sanità, l'istruzione, la previdenza, la pubblica amministrazione, la ricerca, la domotica. Ma in particolare: la comunicazione, i social media, la pubblicità sono i contesti che rilevano maggiormente come le informazioni digitali divenendo dati personali, perché collegate alle persone e sincronizzate con il loro comportamento *online* e *offline,* possano rivelarsi motore di comunicazione, innovazione e sviluppo: *il carburante della nuova economia*[98], al quale però - a differenza di quelli tradizionali come il petrolio, non si può più rinunciare.

Le infografiche di Domo[99] pubblicate periodicamente nell'ambito del progetto *Data never sleeps* fotografano, con rilievo di impatto, la quantità e la tipologia di informazione che ogni minuto viene prodotta e rilasciata *on-line* dagli utenti.

Nell'Aprile 2014 *Data never sleeps 2.0* registra: 4 milioni di ricerche su Google, 204 milioni di email inviate, poco meno di 2,5 milioni di contenuti condivisi su Facebook, 277mila Tweet, 350mila foto su Whatsapp e 48mila app scaricate sui dispositivi Apple[100] (Figura 2.3). A distanza di un biennio, nell'ambito della rilevazione *Data never sleeps 4.0* risultano: 69,5 milioni di parole tradotte da Google Translator, oltre 216mila foto condivise su Facebook, oltre 9mila Emoji scambiati si Twitter, oltre 833mila nuovi upload su Drobox (cfr Figura 2.3).

Nel 2000, la rivista scientifica *Science* stima - sulla base dei rullini venduti su scala mondiale, 100 miliardi di foto scattate all'anno in tutto il mondo, nel 2010 solo in Facebook vengono caricate 2,5 miliardi di foto al mese[101], per passare nel 2014 ad oltre 9miliardi.

---

98 Commissaria UE al mercato interno, Elizbieta Bienkowska, *Ue promuove "economia dei dati"* http://www.ansa.it/sito/notizie/economia/2017/01/10/ue-promuove-economia-dei-dati_42b9f4cd-f065-4446-939e-aa3eb7065702.html (10 Gennaio 2017)
CAVOUKIAN ANN, REED DRUMMOND, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design* (2013) pag. 1

99 In argomento la risorsa è consultabile su: https://www.domo.com/blog/data-never-sleeps-4-0/

100 In argomento il report è consultabile su: https://www.domo.com/learn/data-never-sleeps-2/

101 Cfr Atti Lectio Magistralis Prof. Alessandro Acquisti – *Privacy nell'era del DataGeddon* 19 Giugno 2014, CNR Pisa.

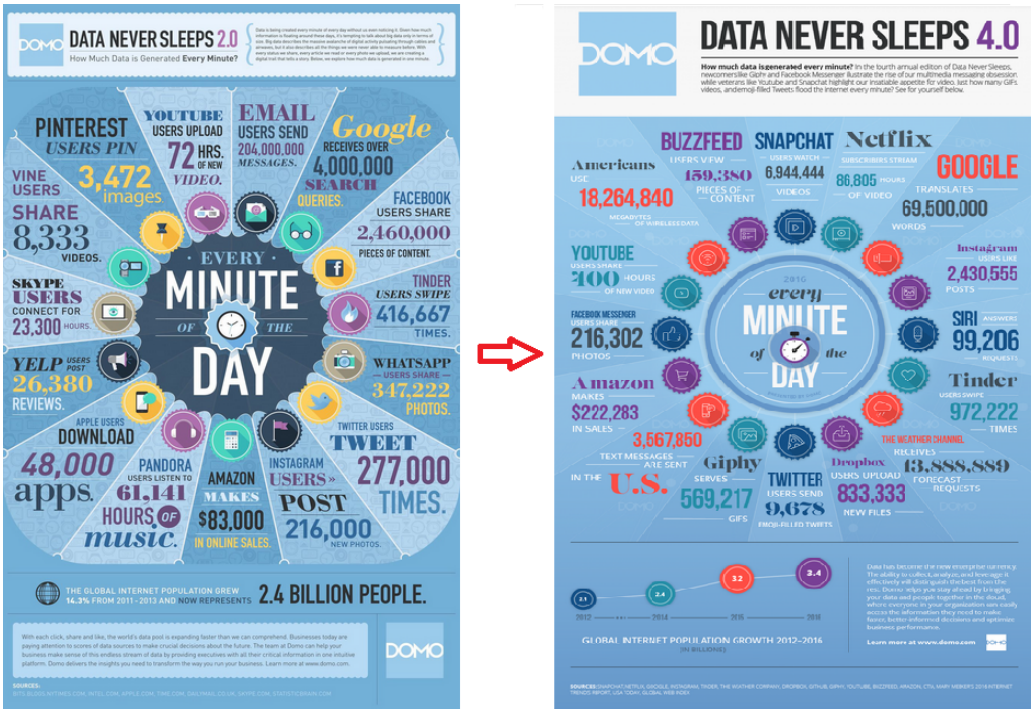


Figura 2.3 – Data Never Sleeps 2.0 (anno 2014) e 4.0 (anno 2016)

Un'indagine di *Global Media Insight*[102] tratta da vari aggregatori statistici nel corso dell'anno 2016, esita la distribuzione degli utenti attivi sui Social Media (su base mensile e aggiornati al 2016) contando: 1609 miliardi di utenti per Facebook, più di un miliardo per YouTube, 950 milioni per WhatsApp e a seguire Google Plus, Instagram, Linkedin.(cfr Figura 2.4).

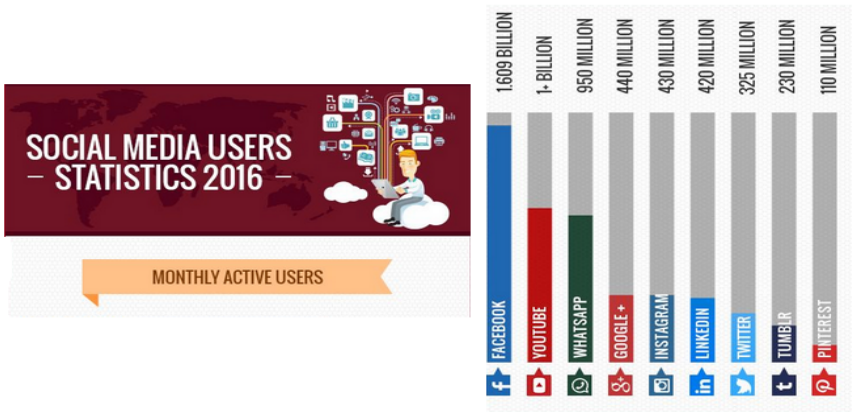


Figura 2.4 – Utenti attivi sui Social Media (su base mensile e aggiornati al 2016)

[102] http://www.globalmediainsight.com/
In argomento la fonte è consultabile su: http://www.4plays.it/social-media-crescono-le-statistiche-2016/

Infine, il settore della pubblicità *on-line* e comportamentale è probabilmente quello che meglio rappresenta come le informazioni sopra elencate - dati di geolocalizzazione, cronologie e dati di navigazione web, ricerche effettuate, condivisioni sui social media, utilizzo di *apps* tematiche su smartphone e tablet, possano essere collegate, sincronizzate, manipolate e incrociate con le informazioni personali disponibili prevalentemente sui social media e rilasciate volontariamente dagli stessi utenti.

Il Financial Times in un digital media del 23 Giugno 2016[103], rileva come nel primo trimestre 2016 per ogni nuovo dollaro investito in *digital advertising* negli Stati Uniti, Facebook e Google abbiano attratto 85 centesimi, grazie al vero e proprio tesoro di dati posseduti, raccolti ad ogni click di *MiPiace* e *Condividi,* interconnessi da servizi diversi[104] e incrociati per modellare comportamenti *online* e *offline* per dedurre dettagliati profili dei loro utenti che, categorizzati, vengono proposti agli inserzionisti per *ads* (annunci) sempre più mirate[105].

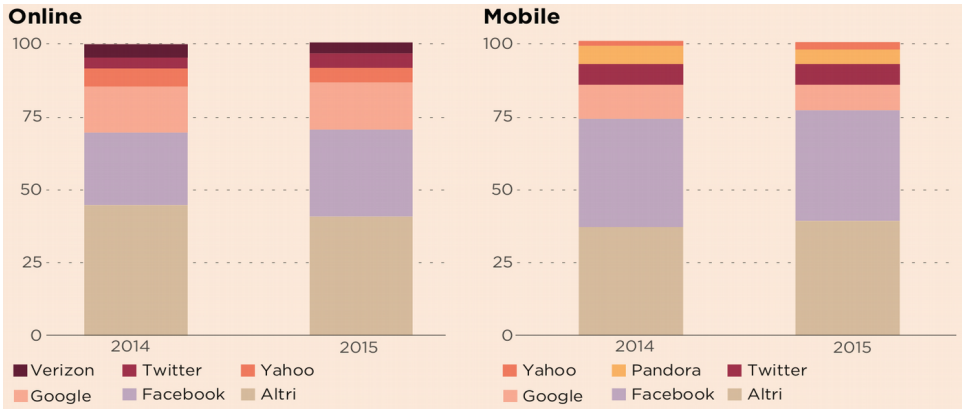


Figura 2.5 – Distribuzione percentuale della quota di mercato della pubblicità on-line tra i principali Social Media (Fonte Pagina99 del 7 gennaio 2017[106])

[103] In argomento la fonte è consultabile su: *Advertising: Facebook and Google build a duopoly* by Matthew Garrahan https://www.ft.com/content/6c6b74a4-3920-11e6-9a05-82a9b15a8ee7 (23 Giugno 2016)

[104] Nel privacy notice del 29 Agosto 2016 Google introduce (tra gli altri) il seguente aggiornamento: *Potremmo unire le informazioni personali derivanti da un servizio a quelle di altri servizi Google (comprese le informazioni personali)* e ancora: *A seconda delle impostazioni dell'account utente, la sua attività su altri siti e app potrebbe essere associata alle relative informazioni personali allo scopo di migliorare i servizi Google e gli annunci pubblicati da Google*. Un "potremmo" tutt'altro che residuale attesa la storica garanzia di Google che i dati sarebbero stati raccolti da DoubleClick (acquistato nel 2007 per 3,1 miliardi di dollari tra molte polemiche proprio per questioni legate alla privacy degli utenti) in forma aggregata e non riconducibili a identità dei singoli utenti. In argomento la fonte è disponibile su: https://www.google.it/intl/it/policies/privacy/archive/20160829/ (29 Agosto 2016)
http://www.pagina99.it/2017/01/11/pubblicita-online-web-advertising-no-tutela-privacy-su-internet-informativa/ (07 Gennaio 2017)

[105] Su questo specifico argomento e sulla centralità dell'utente quale produttore di dati personali si rimanda al successivo paragrafo 1.2 - *La centralità dell'utente nel disclosure dei dati personali* in cui si illustra il ciclo di gestione del processo di *advertising mirato,* dei relativi attori e delle implicazioni in termini di condivisione dei dati personali che coinvolgono ed escludono l'utente.

[106] In argomento la fonte è consultabile su:
http://www.pagina99.it/2017/01/11/pubblicita-online-web-advertising-no-tutela-privacy-su-internet-informativa/ (07 Gennaio 2017)

Al contempo colossi delle telecomunicazioni - come Verizon e IBM, e dell'investimento pubblicitario – come Wapp e Interpublic, tra il 2015 e il 2016 hanno investito dai 4 ai 10 miliardi di dollari, tra investimenti in ricerca e acquisizione nel settore dei dati, per la realizzazione di piattaforme tecnologiche capaci di immagazzinare, aggregare e gestire da fonti diverse dati e informazioni su uno sconfinato dominio di utenti (*mPlatform* di *Wpp);* tutto ciò con lo scopo di intercettare (anticipandole) le informazioni collegate alla proposta di un determinato prodotto in vendita (*Watson Ads* di IBM); oppure per combinare i diversi dati in proprio possesso tra i quali l'indirizzo di posta elettronica, tipo e modello di device utilizzato, l'identificativo univoco del wireless, il numero di carta di credito con i dati di traffico web *(Verizon e Aol)*[107].

Quanto premesso vuole evidenziare, come grandi volumi di informazioni digitali sottoposti a gestione[108], analisi, processamento, interconnessione applicativa e sincronizzazione possano essere qualificati come dati personali[109], divenendo, in quanto tali, motore di nuove forme di valore relazionale, sociale ed economico; di nuovi servizi e di nuove opportunità - per e con al centro la persona, che il linea di principio vengono presentate come tutte positive e a valore aggiunto[110], dipendenti e migliorative della *user-experience.*

In tal senso, lo *"smart-advertising"* (per richiamare la disamina che precede) e i *Social Network* sono solo due degli esempi più rappresentativi e al tempo stesso strettamente interconnessi.; il primo nella sua più migliorativa ed efficace accezione di finalizzare la raccolta e l'analisi di tutte le tracce digitali all'esposizione di servizi di ricerca e predizione altamente personalizzati, efficaci, migliorativi della vita degli utenti e specificatamente centrati su questi in termini di accessibilità, necessità, preferenze ed azioni; il secondo la cui finalità è di migliorare le relazioni e la partecipazione degli utenti.

I settori in cui la gestione dei dati personali genera innovazione e miglioramento variano da quello della sanità con al centro il paziente (si pensi per esempio all'implementazione del Fascicolo Sanitario Elettronico)[111], a quello dell'*e-government* con al centro il cittadino (e in

[107] In argomento la fonte e i dettagli sono consultabili su: http://www.pagina99.it/2017/01/11/pubblicita-online-web-advertising-no-tutela-privacy-su-internet-informativa/ (07 Gennaio 2017)

[108] Per le caratteristiche e la struttura del ciclo di gestione delle informazioni si rimanda al successivo paragrafo 1.1

[109] Per la definizione e le proprietà dei dati personali (digitali) si rimanda al successivo paragrafo 1.1

[110] In argomento si rimanda alle seguenti risorse: Gleick J., *The Information: A History, a Theory, a Flood*. London: Fourth Estate, 2011.

WORLD ECONOMIC FORUM, *Rethinking Personal Data: Strengthening Trust,* http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012)

[111] In argomento si segnala il contributo: MAIOLI C., JORDAN SANCHEZ E. *Big Data e capacità informativa per l'autodeterminazione del paziente,* in Strumenti, Diritti, Regole e Nuove Relazioni di Cura – Il Paziente Europeo protagonista nell'eHealth a cura di Carla Faralli, Raffaella Brighi e Michele Martoni, G. Giappichelli Editore – Torino (2015) p. 155-176

analogia, al Fascicolo Previdenziale o Fiscale), all'istruzione con al centro lo studente[112]; attengono il supporto per la revisione e il *reengineering* di processi, l'eliminazione di inefficienze legate alle duplicazione dei dati; la prevenzione di frodi fiscali legate al mancato o incompleto tracciamento dei flussi informativi.

Su larga scala l'analisi delle informazioni e dei dati personali può supportare una migliore e anticipata comprensione di problemi e di crisi globali come la disoccupazione, l'ambiente, la salute.

La pubblicazione e la condivisione dei dati personali può accelerare il processo di democratizzazione all'accesso all'informazione, coordinare le azioni degli utenti e le relazioni con le persone che condividono interessi simili; responsabilizzarli sul valore delle proprie informazioni e sulle implicazioni di un maggior controllo di utilizzo. Per le organizzazioni governative essere il presupposto per le politiche di sicurezza pubbliche, di contrasto alla criminalità e alla corruzione.

Per le aziende che gestiscono grandi volumi di dati essere, comunque, il volano di innovazione, di nuovi prodotti, di efficienza e crescita economica; indirizzo strategico, vantaggio competitivo.

Questo scenario di opportunità, sintetico quanto non esaustivo, non è privo di resistenze che possano limitarne o comprometterne le potenzialità, introducendo quindi dei *trade-off* nella gestione delle informazioni personali tra i vantaggi e le criticità che ne conseguono e che lo sviluppo delle *ICT* illustrate ha esacerbato agendo come catalizzatore di ulteriori tecnologie volte tanto a supporto e a miglioramento dei sistemi di gestione delle informazioni tanto alla protezione (o alla violazione) delle informazioni stesse.

Da un lato persone, imprese e istituzioni vogliono conoscere quanto più è possibile dei soggetti di cui trattano le informazioni sottovalutando gli effetti controproducenti dell'eccesso di interferenza nella sfera ritenuta *privata;* dall'altro nelle persone si mantiene vivo e crescente l'interesse e il bisogno di rivelare informazioni personali per ottenere servizi migliori, per una naturale esigenza di comunicazione, di apertura, ed di interazione auspicando che tali informazioni non vengano sfruttare abusivamente o in maniera dannosa. Tutt'altra che secondaria, inoltre, la sollecitazione economica: come evidenziato per lo "*smart-advertising*" e i

[112] In tutti i casi gli utenti, quando la profilazione che sia sanitaria, sociale, formativa - se autorevole, veritiera e di qualità, oltre che alimentarla ricevono un ritorno vantaggioso in termini di opzioni di accesso alle informazioni, differenziate, complete e riutilizzabili; semplificando così il diritto di autodeterminazione.

Social Media, lo sviluppo e le potenzialità *analytics* connesse alla gestione dei dati personali in realtà nasconde ragioni di profitto dietro le giustificazioni virtuosamente orientate al migliorare la vita delle persone.

L'effetto d'insieme delle moderne tecnologie può rendere la vita molto comoda, ma anche completamente visibile e trasparente ad osservatori sconosciuti. Il volume di dati veicolato può – tanto ad opera di aziende tanto di singoli soggetti può essere acquisito, conservato, confrontato, collegato, combinato, manipolato per dedurre con tecniche di *data mining* – a velocità crescenti e costi sempre più bassi, stime accurate, profili dettagliati o report completi del comportamento e delle attività di ogni individuo senza che questi ne sia a conoscenza e men che meno abbia rilasciato la propria autorizzazione.

Tutti gli attori coinvolti, seppur in forme e misure diverse, condividono perplessità, sospetto, diffidenza, dubbi o paure su come i dati personali sono gestiti; ciò anche a causa dei possibili rischi, delle minacce e delle effettive violazioni occorrenti nell'utilizzo, che traducono le preoccupazioni in erosione e perdita di fiducia. Tra gli utenti, in particolare, ricorre una disconnessione tra le preoccupazioni su come sono gestite e trasferite le proprie informazioni, l'attitudine alla protezione e l'effettivo comportamento.

Su questa questione, rilevante per il valore non solo informativo ma sostanziale delle informazioni personali, convergono vari fattori:

- ✔ la natura e le caratteristiche intrinseche dei dati personali digitali – la quantità, la dinamicità e l'ubiquità;
- ✔ gli attori coinvolti e le relative aspettative in termini di utilizzabilità delle informazioni;
- ✔ le opportunità, gli interessi (anche contrapposti) e il bilanciamento con le relative criticità;
- ✔ il conflitto - crescente negli utenti ai quali le informazioni personali si riferiscono, connesso al dover condividere con altri attori (titolari, responsabili, fornitori di servizi, altri utenti, e oggi sempre in misura maggiore dispositivi) le regole di utilizzo, di processamento ma soprattutto di sfruttamento economico dei propri dati personali in assenza di uno speculare vincolo di *proprietà* e di un contingente requisito di *possesso;* nonché di efficaci strumenti – effettivamente utilizzabili dall'utente nei casi un cui chi gestisce le informazioni omette trasparenza e/o preclude il controllo esercitabile dall'utente volto a limitare o opporre l'analisi e la profilazione nelle sue abitudini e delle

sue prerogative personali[113].

Oltre alle tradizionali minacce e ai tradizionali rischi opposte dalla sicurezza delle informazioni digitali, quali sono quelle che specificatamente attengono le informazioni personali e quali sono i presupposti di tali rischi?

In quali forme e con quali modalità, il trattamento su larga scala dei dati personali può erodere la vita privata, la sfera individuale e i valori intrinseci che caratterizzano la persona

Quali sono i fattori che favoriscono e condizionano un maggiore *disclosure* dei dati da parte degli utenti, aumentando quindi tale potenziale di erosione?

Chi sono i *legittimi* proprietari dei dati personali rilasciati volontariamente dagli utenti o ad essi comunque riconducibili a seguito di trattamento, analisi, collegamento, deduzione?

Qual'è l'effettivo valore dei dati personali e della privacy,?

[113] Sull'argomento si indicano le azioni intraprese dal Garante Privacy Italiano nell'ambito della c.d. Cookie Law e disponibili alle seguenti risorse.
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015 2014, G.U. n. 103 del 6 maggio 2015
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4020961

1.1. LE PROPRIETÀ DEL DATO PERSONALE, LA GESTIONE E GLI ATTORI COINVOLTI.

I dati personali sono 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, ecc.[114], laddove per identificazione – avvenuta o da venire, si intende la distinguibilità di una persona dalle altre.

Molti dati personali sono associati nativamente alla persona (dati identificati o identificatori come il nome, la foto, caratteri fisiologici); altri sono volontariamente forniti dall'utente (*Volunteered Personal Information*[115] come dati di account, recapiti e riferimenti on-line, ma anche connesse ad azioni compiute, come acquisti e ricerche); altre informazioni concorrono all'identificazione se combinate insieme (ad esempio quelle che descrivono il profilo e le attività in rete, il contesto, il profilo sanitario, professionale economico, etc.).

Possiamo rappresentare le informazioni personali nella loro voluminosità come una sorta di sfere concentriche disposte a strati come quelli di una *cipolla* e proiettati verso l'utente che le produce o a cui si riferiscono identificandolo direttamente o indirettamente.

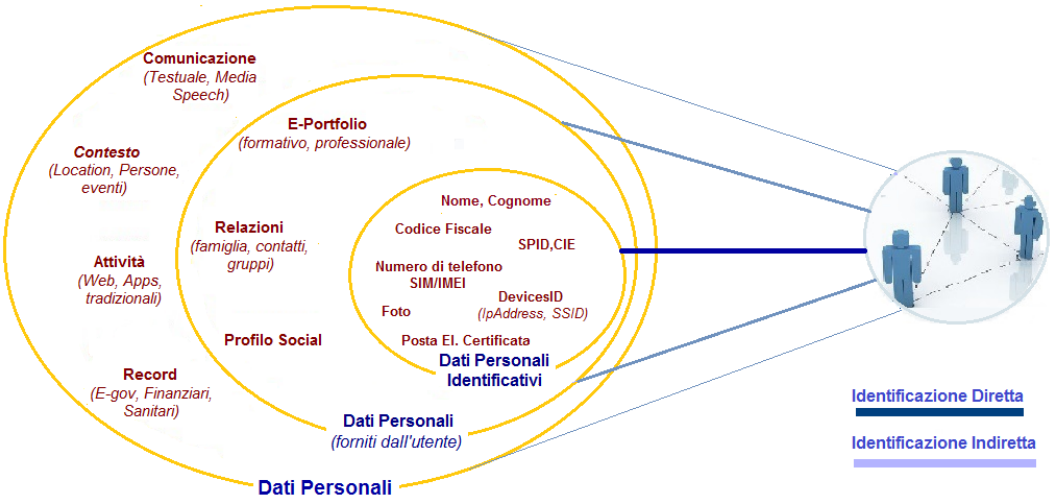


Figura 2.6 – Tipologie di dati personali e identificabilità della persona

Una persona può essere identificata direttamente attraverso il nome o indirettamente attraverso una combinazione di criteri significativi che ne consentano il riconoscimento e la distinzione all'interno del gruppo al quale appartiene. Il nome è l'identificatore più comune, nella pratica l'avvenuta identificazione di una persona implica un riferimento al suo nome anche se proveniente da altri identificatori quali il numero di telefono, il codice fiscale, la carta di identità elettronica.

[114] http://www.garanteprivacy.it/web/guest/home/diritti/cosa-intendiamo-per-dati-personali

[115] Questa tipologia di dati personali viene denominata *Volunteered Personal Information* (*VPI*) Ctrl-Shift, https://www.ctrl-shift.co.uk/tag/volunteered-personal-information/

La sfera più vicina all'utente contiene i dati identificativi collegati all'interessato direttamente, senza ulteriori informazioni di tramite. Quella intermedia contiene informazioni prodotte dall'utente nel corso della propria *on-line experience* e strutturate mediante l'intervento applicativo di terze parti nell'ambito di un processo di trattamento. L'ultima e più esterna contiene prevalentemente informazioni di trattamento, risultato non solo di aggregazione (come per la sfera intermedia) ma di relazione semantica, analisi e inferenze che producono ulteriore informazione, nuova e diversa rispetto a quella prodotta e rilasciata in origine dal soggetto interessato.

Quest'ultimo dominio nella sua generalità e piena estensione configura un trattamento di *schema Big Data* che in dettaglio sarà oggetto di descrizione nel capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.*

Procedendo dall'utente verso la sfera più esterna, *controllo* e *possesso* dei dati personali - tra l'utente che le produce e terze parti (titolari, stakeholders) che le trattano e le sfruttano - sono inversamente proporzionali. Più le informazioni personali sono lontane dell'utente più questi ne avverte la perdita di controllo che parallelamente passa agli attori che ne gestiscono il trattamento.

Le proprietà principali del dato personale sono ancorate alla sua definizione sulla quale convergono sia la declinazione tecnica introdotta dallo standard ISO/IEC 29100:2011[116]:

- ✔ un *PII (Personal Identifiable Information):* qualsiasi informazione che a) può essere utilizzata per identificare il soggetto interessato al quale tale informazione di riferisce oppure b) è o potrebbe essere direttamente o indirettamente collegata al soggetto interessato.

sia quella normativa richiamata nel GDPR, all'art. 4 *Definizioni*, comma 1 :

- ✔ «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;

Le proprietà estraibili dalle definizioni che connotano il dato personale e che lo collegano alla

[116] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*, 15 Dicembre 2011 (First Edition) p. 8

persona interessata sono principalmente tre:

1. l'essere informazioni in quanto tali – indipendentemente dal concernere una determinata persona, dall'identificarla o dall'essere o meno corrette; sono distinte da una natura oggettiva (ad esempio un carattere fisiologico, biometrico, biologico) oppure soggettiva (una opinione, una valutazione); da un contenuto (ad esempio attinente la vita privata o professionale); e dal formato (ad esempio testuale, grafico, fotografico, sonoro). In questo ambito si parla di informazioni, non di soggetti e non di persone.

2. Il *concernere* nel senso di *riguardare* una persona – indipendentemente dall'identificarla: stabilire la presenza di questo requisito spesso è immediato, ad esempio le informazioni di un fascicolo sanitario concernono (banalmente) il paziente; ma non si rivela altrettanto immediato laddove questo requisito è connesso inizialmente ad un oggetto (ad esempio l'informazione rappresentate il valore di un immobile o la velocità di un veicolo) e solo successivamente *concernere* l'interessato (ad esempio quando questa informazione viene connessa ad una fascia di reddito del proprietario, o allo stile di guida di un guidatore). Le informazioni possono variamente concernere un soggetto a seconda del contenuto, della finalità e dell'impatto[117]. In questo ambito si parla di informazioni e di soggetti ma non di persone.

3. Infine, l'identificazione o identificabilità (quest'ultima diretta o indiretta) è la proprietà che qualifica e caratterizza l'*informazione* come *dato personale;* da un punto di vista logico può essere intesa come una relazione biunivoca di attribuzione (e quindi si distinzione), tra il dominio delle possibili informazioni concernenti i soggetti e l'insieme delle persone.

   Questa relazione è diretta quando è immediata e/o non necessita di ulteriori passaggi deduttivi per distinguere univocamente la persona[118]; l'unicità dell'informazione favorisce questa caratteristica così come il fatto che determinate informazioni siano fornite volontariamente e direttamente dalla persona interessata *(VPI)*. L'identificazione o l'identificabilità indiretta rimanda, in genere, al computo di

[117] In argomento, per un maggiore dettaglio ed esempi si rimanda al parere Working Party ex art. 29 n. 136, 20 June 2007, *Opinion 4/2007 on the concept of personal data* (IT) p. 10-12

[118] In argomento sia il CODICE che lo standard ISO/IEC 29100:2011 convergono nello specificare, rispettivamente tramite il *dato identificativo* e l'*identifier*, una tipologia di dato personale con identificazione diretta.
CODICE, Art. 4 - Definizioni, comma 1, lettera c): *"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato* ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*, 15 Dicembre 2011 (First Edition) p. 7

combinazioni uniche, ampie o ridotte. Nei casi in cui gli identificatori disponibili non consentono di identificare una specifica persona, la si può ancora considerare *identificabile* se tali informazioni combinate con altre consentiranno di distinguerla.

Questo requisito dipende fortemente dal contesto di riferimento: in generale che un dato personale identifichi una persona di per se non è ne una condizione necessaria ne una condizione sufficiente; ad esempio il dato personale *nome* può (con molta probabilità) identificare immediatamente la persona_studente nell'ambito di un'aula (e in questo contesto rivelarsi dato identificativo) ma non altrettanto direttamente nell'ambito di una Università essendo necessarie ulteriori informazioni in ragione delle possibili omonimie.

Inoltre la possibilità di identificare la persona non presuppone necessariamente di disporre del *nome,* essendone possibile la ricostruzione della personalità/persona o del profilo attraverso la categorizzazione basata su criteri socioeconomici, fisiologici, professionali, di relazione, di localizzazione, considerato tra l'altro che il punto di contatto (il *device*) tra l'utente e la rete, di per se, non richiede necessariamente che ne sia svelata l'identità in senso stretto. L'identificabilità della persona, infine, va misurata tenendo presente l'insieme dei mezzi ragionevolmente utilizzabili[119]. La sola possibilità ipotetica di distinguere una persona non basta per considerare tale persona *identificabile*. Se, tenendo conto dell'*insieme dei mezzi che possono essere ragionevolmente per identificare detta persona,* tale possibilità non esiste o è trascurabile, la persona non dovrebbe essere considerata *identificabile,* e le informazioni non configurerebbero *dati personali.*

Il criterio di valutazione deve tenere conto di diversi fattori in gioco: il costo dell'identificazione, la finalità, le caratteristiche della gestione e del trattamento e l'arco temporale degli stessi; il rischio di disfunzioni organizzative (es. violazioni degli obblighi di riservatezza) e tecniche. Questa valutazione dipende dinamicamente dal contingente stato dell'arte della tecnologia al momento del trattamento e dalle possibilità di sviluppo nel periodo per il quale saranno trattati e conservati i dati.

La gestione dei tati personali è declinata in maniera essenziale ma esaustiva nella definizione stessa di *trattamento* richiamata dal GDPR all'art. 4 *Definizioni*, comma 2:

[119] GDPR, considerando 26): *dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.*

- ✔ «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

La schematizzazione del ciclo di vita (o di gestione, di trattamento) dei dati personali trova immediato adattamento nel classico ciclo di vita dell'informazione, che di norma include le seguenti fasi[120]:

- ✔ l'*occorrenza* in cui si collocano la scoperta, il design, la creazione...;
- ✔ la *trasmissione* in cui convergono il rilascio, la condivisione in rete, la distribuzione, l'accesso, il recupero, la diffusione....;
- ✔ il *processo* e *la gestione:* risultante della raccolta, validazione, modifica, organizzazione, indicizzazione, classificazione, filtro, aggiornamento, archiviazione,...;
- ✔ l'*utilizzo* comprendente tra l'altro il monitoraggio, l'interpretazione, la modellazione, l'analisi, la previsione, la decisione....;

sulle quali, con immediatezza, possono essere collocate tutte le operazioni di trattamento (cfr successiva figura 2.7).

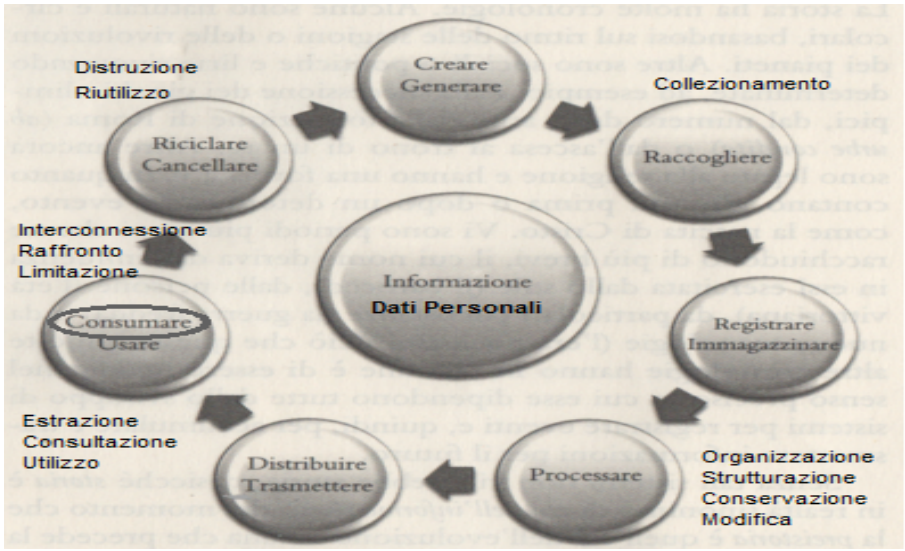


Figura 2.7 – Il tipico ciclo di vita dell'informazione adattato al trattamento dei dati personali

[120] cfr LUCIANO FLORIDI, *La rivoluzione dell'Informazione*, Codice Edizioni p. 4 -5

La strutturazione delle fasi dipende dall'intrinseca natura intangibile del dati personali digitali; questa implica che essi – come tutte le informazioni digitali possano implementare il c.d. *Data-Accretion*[121], quindi:

- ✔ possano essere copiati infinitamente, distribuiti globalmente abbattendo limitazioni e costi tradizionalmente associate ai manufatti informativi tangibili (materiali e cartacei);
- ✔ inoltre a differenza di questi ultimi l'utilizzo dei dati digitali non implica consumo (nel senso dell'esaurimento), ma riutilizzo che produce (a sua volta) ulteriore conoscenza, e quindi ulteriori dati;
- ✔ ed infine la connessione, il collegamento e la relazione di insiemi di dati personali ne moltiplica la quantità.

Queste caratteristiche native dei dati personali digitali sono quelle da cui originano tutte le tipologie di sfruttamento positivo premesse al paragrafo precedente; ma – unitamente alla centralità rivestita dell'utente nel *disclosure,* nella divulgazione delle proprie informazioni, sono quelle da cui derivano le vulnerabilità dei sistemi di trattamento rispetto alle molteplici situazioni in cui gli attori coinvolti – ed in particolare il soggetto interessato, ne perdono – a rilascio avvenuto, il totale controllo.

Anche sulla definizione degli **attori coinvolti** nel ciclo di gestione e di trattamento dei dati personali si può registrare una sostanziale convergenza, almeno per le tipologie, tra le indicazioni tecniche esposta nello standard ISO/IEC 29100:2011 e quelle normative normativa incluse nel GDPR. Lo standard ISO/IEC 29100:2011 prevede che nel trattamento dei dati personali siano coinvolti 4 tipi di attori: il *PII principal*, il *PII controller*, il *PII processor* e le terze parti[122]. Nel nuovo regolamento europeo alle prime tre figure corrispondono: il soggetto interessato, il titolare del trattamento e il responsabile del trattamento ai quali si affianca anche un quarto e nuovo attore: il responsabile per la protezione dei dati personali (*Data Protection Officer*, *Privcay Officer*).

Il *PII principal* – *Soggetto Interessato* è la persona fisica ai quali si riferiscono i *PII (Personal Identifiable Information)*: laddove non è previsto di default dalla legge fornisce le proprie informazioni personali sia al *PII controller*, che al *PII processor*; rilascia il proprio consenso e imposta le opzioni di processamento e di trattamento rispetto alle politiche e alle regole predefinite ed esposte dal *PII controller*. Oltre al consenso esercita un insieme di diritti

[121] Atti Lectio Magistralis Prof. Alessandro Acquisti – *Privacy nell'era del DataGeddon* 19 Giugno 2014, CNR Pisa.

[122] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*, 15 Dicembre 2011 (First Edition) p. 5

predefiniti dalle norme regolatorie (ad esempio il diritto di accesso, di limitazione, di rettifica, modifica e cancellazione) quali strumenti di controllo sulle proprie informazioni.

Il *PII controller – Titolare del trattamento* (o il contitolare, potendo contarne più di uno) è il portatore di interesse che determina le finalità (i perché) e i mezzi (come) del trattamento dei *PII*; secondo lo standard rientra in questa categoria anche la persona che tratta le informazioni per scopi personali, non altrettanto nel nuovo Regolamento Europeo. Il *PII Controller* è tenuto a comprovare la sua responsabilità nell'adottare e nel mettere in atto tutte le misure organizzative e tecniche (ivi incluse quelle di sicurezza e di valutazione dell'impatto e prevenzione dei rischi) perché il trattamento soddisfi e rispetti in modo efficace i principi di protezione dei dati e includa tutte le garanzie necessarie per tutelare i diritti dei soggetti interessati.

PII processor - Responsabile del trattamento è il portatore di interesse che tratta i dati per conto del *PII controller*. Monitora il rispetto ai requisiti dello standard o del regolamento e implementa i relativi controlli. Nel nuovo regolamento europeo, che assegna al responsabile un ruolo quasi in solido con il titolare, è supportato e coadiuvato dal responsabile per la protezione dei dati personali.

E in fine le *terze parti* sono i portatori di interesse diversi dalle precedenti figure che trattano i dati sotto il controllo del titolare e del responsabile.

1.2. LA CENTRALITÀ DELL'UTENTE NEL *DISCLOSURE* DEI DATI PERSONALI.

Al fine di evidenziare la asimmetria e lo sbilanciamento di ruolo e di informazioni gestite e sfruttate - tra l'utente, attore centrale e produttore di dati personali, e gli *stakeholders* che li commercializzano e li sfruttano si ritiene utile riportare gli esiti di un caso di studio divulgato in un report del Web Economic Forum prodotto nell'ambito di un'indagine svoltasi tra il 2012 e il 2014 volta ad investigare le ragioni tanto della disponibilità tanto del distacco e dell'erosione di fiducia dell'utente al rilascio e alla divulgazione delle proprie informazioni[123].

Senza, per il momento entrare nel merito nel complesso di vulnerabilità, di minacce e dei possibili rischi che ne conseguono e quindi delle questioni attinenti la protezione dei dati personali, per le quali si rimanda al successivo paragrafo 2.3 - *Protezione dei dati personali: le criticità e i rischi connessi alla gestione,* l'obiettivo è quello di focalizzare l'attenzione illustrando un caso pratico descrittivo delle fasi del ciclo di vita delle informazioni attinenti la creazione, il rilascio, la raccolta e il riutilizzo.

Questo caso di studio illustra come il rilascio dei dati personali da parte dell'utente, oltre ai casi in cui la registrazione ad un servizio è passaggio necessario e obbligatorio per poterne fruire, possa essere direzionato e controbilanciato da altri benefici tangibili: la personalizzazione di un servizio, trattamenti preferenziali, sconti, premi compensazioni monetarie. Processo al quale l'utente potrebbe: *i)* opporsi, per esempio rifiutandosi di fornire certe informazioni con conseguente negazione del servizio; oppure, *ii)* limitare, rilasciando dati falsi precludendo, però, ritorni di personalizzazione; od ancora *iii)* controllare, adottando contromisure di sicurezza o di *privacy;* o, infine, *iv)* subirne a posteriori eventuali violazioni.

Sull'argomento, significativa e tutt'ora valida, si rivela l'interpretazione di Varian (1996)[124] che paragona il rilascio di dati personali alla firma di un *assegno in bianco* da parte dell'utente. L'informazione rivelata durante una transazione potrebbe essere utilizzata per fornire il miglior servizio al consumatore, ma potrebbe implicare anche negatività che variano da errori

[123] L'indagine del WEF è descritta in 4 documenti:
World Economic Forum, Rethinking Personal Data: Strengthening Trust, http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012)
World Economic Forum, Unlocking the Value of Personal Data: From Collection to Usage, http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage (2013),
World Economic Forum, Rethinking Personal Data: A New Lens for Strengthening Trust, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf (2014)
World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (2014)

[124] VARIAN H.R., *Economic Aspects of Personal Privacy,* Privacy and Self-regulation in the Information Age, National Telecommunications and Information Administration, 1996, p. 1

involontari nell'utilizzo dei dati, alla semplice influenza; dalla discriminazione al ricatto. Tutte conseguenze che derivano dalla rivelazione volontaria di dati personali ma che l'utente è raramente in grado di valutare e prevedere.

Questo caso di studio è utile, inoltre, ad evidenziare come le questioni che riguardano la *privacy* e la protezione dei dati personali per essere inquadrate in maniera corretta ed esaustiva necessitano di riflessioni in due aree collegate ma distinte: da un lato quella delle informazioni personali, con le associate proprietà e il relativo mercato (e a queste argomentazioni è dedicata la prima parte del presente capitolo); e dall'altra quella del controllo di tali informazioni. La prima area, con riferimento al caso illustrato, è quella in cui si possono collocare i *data marketers* e i *data miners* e la seconda quella a cui si riferiscono le tecnologie e i frameworks di protezione dei dati personali.

Il processo coinvolge una filiera di 10 attori: l'utente interessato e il relativo *data aggregator,* il *publisher,* il *data marketer,* l'*attribute verifier,* il *data analytics provider,* l'*aggregated data set broker,* il *retailer,* il *network address provider,* il *payment processor.*

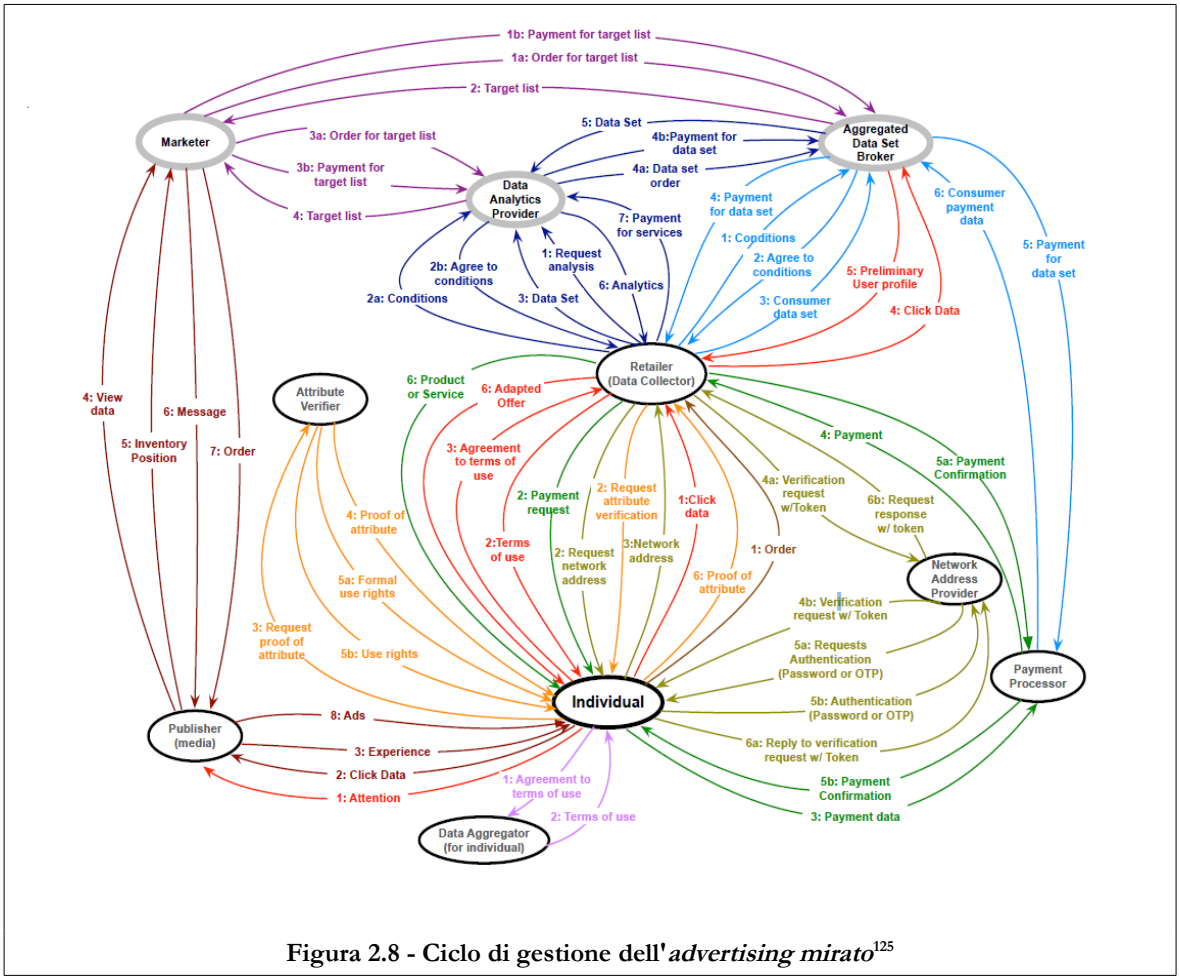


Figura 2.8 - Ciclo di gestione dell'*advertising mirato*[125]

1. L'utente richiede la visualizzazione di un annuncio sul sito del *publisher;* accetta l'utilizzo di cookies analitici e di profilazione; rilascia le informazioni identificative richieste;
2. la richiesta viene rediretta al *marketer* che confeziona un messaggio di annuncio proponendolo all'utente;
3. persuaso dall'annuncio, l'utente richiede la corrispondente offerta sul sito del rivenditore;
4. il rivenditore rigira la richiesta comprensiva di metadati (ad esempio indirizzo IP e localizzazione) al *broker* aggregatore di dati che configura un primo profilo dell'utente rilasciandolo al rivenditore;
5. il rivenditore utilizza tale profilo per meglio personalizzare l'offerta;
6. l'utente accetta l'offerta e opta per un prodotto che richiede una prova di attributo (ad esempio comunicazione dello status o dell'età), informazione che condivide con il rivenditore;
7. il rivenditore richiede anche un valido *end-point* di contatto con l'utente, che condivide con il *network address provider;*
8. il rivenditore associa l'utente ad processore di pagamento. A transazione ultimata l'utente riceverà il prodotto ordinato.

Il rivenditore detiene un set di dati personali e di transazione che rivende al *broker* aggregatore di dati; richiede un'analisi dei dati ad un *data analytics provider* che acquista i dati dal *broker* aggregatore di dati. Il *marketer* acquista i dati sia dal *broker* aggregatore dei dati che dal *data analytics provider* per perfezionare il modello dei successivi annunci da proporre all'utente.

L'utente non ha nessuna inter-relazione con il *marketer,* il *broker* aggregatore di dati, e il *data analytics provider,* i quali collezionano, detengono i dati personali dell'utente, li studiano e li analizzano per fare d*ata-accretion*: dedurre un profilo dell'utente che consenta di configurare un prodotto mirato, amichevole e familiare, che comunica direttamente all'utente e verso il quale questi ha una naturale predisposizione positiva; il tutto senza che l'utente sia consciamente informato di ciò che sta capitando.

[125] Fonte: Verna Allee of Value Network LLC, in collaborazione con *Personal Data Ecosystem Consortium*

1.3. RIPENSARE IL CONCETTO DI DATO PERSONALE.

La definizione di dato personale tanto nelle evidenze regolatorie tecniche che giuridiche è strettamente legata alla relazione di attribuzione e di identificabilità con la persona (cfr precedente paragrafo 1.1- *Le proprietà, la gestione e gli attori coinvolti.*

Il trattamento di questa particolare categoria di informazioni comprende di fatto la totalità delle operazioni possibili, nel superiore vincolo che tali operazioni siano lecite e legittime, che presuppongano, implichino e garantiscano il rispetto della protezione dei dati personali, oltre alla tutela degli altri diritti e libertà fondamentali per la persona.

Al centro quindi vi è la persona - identificata dal dato personale, e la tutela dei suoi diritti fondamentali.

Affinché ciò possa avvenire l'impianto regolatorio si basa sul predefinire e mappare (a priori) una serie di diritti per gli interessati (dettagliati nel capitolo 1), una serie di responsabilità/doveri per il titolare e il responsabile e una serie di strumenti: il consenso, l'informativa, l'utilizzo dei dati (parimenti disaminati nel capitolo 1).

Nonostante il nuovo Regolamento Europeo abbia introdotto novità significative orientate a conferire al soggetto interessato un maggior controllo sulle proprie informazioni[126] il carattere di questo impianto regolatorio rimane la generalità e la pre-definizione.

Una generalità che stenta a tradursi in flessibilità e robustezza, rallentando la sua portata in contesti *data intensive* - in cui è intrinsecamente complicato prevederne e gestirne a priori finalità ed utilizzi, traducendosi di fatto in una staticità centrata sulla responsabilità del titolare e ferma sulle condizioni iniziali di raccolta delle informazioni.

Questo aspetto - durante il susseguirsi delle proposte, lo svolgersi dell'iter di elaborazione del nuovo Regolamento e della ricognizione dei suggerimenti per una efficace riforma della Direttiva n. 95/46/CE, è stato argomentato in diversi lavori di ricerca[127] ed in

[126] Su questo aspetto si richiamano: l'inequivocabilità del consenso, i nuovi trattamenti quali la profilazione, le nuove contromisure preventive come il *privacy by design* e la valutazione di impatto, i nuovi diritti come l'oblio e la portabilità dei dati.

[127] In argomento si segnala:
NUNO NORBERTO, DE ANDRADE GOMES, *Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights,* Privacy and Identity Management for Life, Volume 352 of the series IFIP Advances in Information and Communication Technology p. 90-107 (2011), par. 3 p. 101 – 104

WORLD ECONOMIC FORUM, *Rethinking Personal Data: Strengthening Trust* http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012), p. 15-21

WORLD ECONOMIC FORUM, *Rethinking Personal Data: A New Lens for Strengthening Trust,* http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf (2014), p.11-15

WORLD ECONOMIC FORUM, *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems,*

particolare nei pareri e nelle raccomandazioni del Working Party ex art. 29[128] originando interrogativi su come la definizione *ex-ante* di diritti e responsabilità potesse essere esaustiva a ricoprire tutti i possibili tipi di dati personali e soprattutto tutti i possibili utilizzi non preventivabili a priori; con quali costi, e con quale impatto per l'innovazione e la creazione di valore in una dimensione di efficace ed effettiva libera circolazione delle informazioni e bilanciamento di contingenti (e opposti) interessi di tutti gli attori in gioco.

La limitazione è connessa al fatto che la concettualizzazione di dato personale è legata ad una definizione assolutamente generale, ad una altrettanto ampia definizione di trattamento ma al contempo ad un'assenza di modellazione legata alla finalità (se non per la sommaria distinzione in finalità primarie e secondarie) e alla tipologia di dato (cfr successivo paragrafo 1.4 - *La modellazione dei dati personali.*)

La risposta – secondo le fonti disamine in letteratura[129], potrebbe essere rintracciata nel modellare il dato personale in un contesto parametrizzato dagli stessi dati piuttosto che dalle caratteristiche di trattamento, rendendo così possibile configurare diritti, responsabilità e quindi permessi (intesi quali azioni applicative di diritti e responsabilità) in maniera adattabile, flessibile ma soprattutto dinamicamente dipendente dalle finalità e dall'utilizzo.

A livello definitorio il dato personale potrebbe quindi essere ripensato e inteso come:

- ✔ *l'insieme dei dati e dei metadati relativi ad una persona identificata o identificabile,* laddove per metadati si intende la formalizzazione di alcune native caratteristiche dei dati personali proprie degli ambienti interconnessi; *un insieme di attributi descrittori che consentono l'arricchimento dei dati su base semantica configurando il c.d. schema di trattamento Big Data[130],*

http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (2014), p. 4-12

[128] In argomento si segnala:
WP 199, 05 October 2012, Opinion 08/2012 *providing further input on the data protection reform discussions*
WP 191, 23 March 2012, Opinion 01/2012 *on the data protection reform proposals*
WP 187, 13 July 2011, Opinion 15/2011 *on the definition of consent*
WP 43, 17 May 2001, Recommendation 2/2001 o*n certain minimum requirements for collecting personal data on-line in the European Union*

[129] Con riferimento agli approcci *context-dependent* che intervengono nella definizione delle contromisure a garanzia della protezione dei dati personali, il presente elaborato ne ha disaminato caratteristiche e applicabilità nell'ambito della definizione dei framework delle politiche d'uso dei dati personali finalizzate al loro controllo. Questo argomento è incluso e trattato nel capitolo 3 - *Privacy e Protezione dei Dati personali: le contromisure.* Tuttavia nell'ambito delle fonti consultate è stato possibile estrapolare dei criteri di modellazione attinenti il dato personale rispetto ai contesti informazionali in cui può essere connotato. Su questo argomento le principali fonti consultate ed elencate in bibliografia sono:

XIAODONG JIANG, LANDAY J.A., *Modeling privacy control in context-aware systems* (2002)

HENRICKSEN K., WISHART R., MCFADDEN T., INDULSKA J., *Extending context models for privacy in pervasive computing environments* (2005)

QINGSHENG ZHANG ET AL., *A Study on Context-aware Privacy Protection for Personal Information* (2007)

SHORT STUART, KALUVURI SAMUEL PAUL, *A Data-Centric Approach for Privacy-Aware Business Process Enablement* (2011)

KELBERT FLORIAN, PRETSCHNER ALEXANDER, *Data usage control enforcement in distributed systems* (2013)

[130] L'argomento è stato approfondito al capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.*

Una rielaborata concettualizzazione del dato personale basata sulle caratteristiche sopra indicate può rivelarsi vantaggiosa per più di una motivazione:

- ✔ concorre a bilanciare a priori – tra tutti gli attori coinvolti, utilizzi e rischi, diritti e responsabilità di trattamento, favorendo una efficace conversione in politiche, regole e permessi di utilizzo alla cui configurazione il soggetto interessato può esercitare un ruolo un più attivo e consapevole;
- ✔ può essere immediatamente affiancata e quindi risultare complementare ai criteri di modellazione associati a caratteristiche assunte dal dato personale in conseguenza del suo trattamento: quindi a seconda delle finalità primarie e secondarie; e della tipologia per coefficiente di confidenzialità;
- ✔ la flessibilità intrinseca del contesto può tradursi nell'esporre all'utente un consenso altrettanto dinamico al variare degli utilizzi e delle finalità, effettivamente informato perché più semplice, immediato, tangibile nelle implicazioni, chiaro, visibile, ed efficace e tale da dirigere l'attenzione dell'utente oltre la scelta binaria accetto/declino; instaurando un canale di interesse e di valutazione consapevole, quindi di fiducia, che sia coerente, effettivo e durevole;
- ✔ la diversa caratterizzazione può differenziare permessi e autorizzazioni sulle operazioni di cancellazione, copia, trasferimento e portabilità dei dati personali; operazioni sulle quali è necessario siano bilanciati diritti e responsabità tanto dei titolari quanto dei soggetti interessati, per non privare i primi di una risorsa di valore e i secondi di una contromisura verso trattamenti ritenuti non leciti, non corrispondenti alle proprie necessità e alle proprie scelte, o comunque sucettibili di revisione e riesame.

1.4. LA MODELLAZIONE DEI DATI PERSONALI.

I criteri di modellazione dei dati personali rilevati in letteratura rispondono ai due approcci illustrati rispettivamente nei precedenti paragrafi 1.1. e 1.3.: quello legato alla portata identificativa mutuato dall'attuale normativa e dallo standard ISO/IEC 29000:2001 sulla protezione dei dati personali e quello legato alla riconcettualizzazione del dato personale (ancora in fase embrionale) dipendente dal contesto.

Gli esiti delle due modellazioni sono complementari e diversi sia dal punto di vista formale che per gli scenari informativi che veicolano.

In base al primo approccio[131] il dato personale o *PII* (*Personal Identifiable Information*) può essere modellato con la seguente categorizzazione:

- ✔ record contenente un *dato identificativo*[132];
- ✔ *pseudonimo* il cui valori identificativi è stato oscurato[133];
- ✔ *metadato* ovvero un dato personale di natura applicativa incluso anche in maniera non visibile in documenti o in report;
- ✔ dato personale, distinto al variare del coefficiente di confidenzialià in: dato pubblico, dato privato, dato sensibile;

Il secondo approccio, diversamente, categorizza i dati personali rispetto ai tipici contesti di utilizzo di uno scenario informativo interconnesso su diverse applicazioni e su diversi servizi, come rappresentato nella figura 2.9 – *Mappa di dati personali,* in cui i nodi principali della mappa: *Health Data, Communications, Activity, Content, Context, Identity, Asset Data, Relationships, ePortfolio e Government Records* puntano ad evidenziare come una nuova riconcettualizzazione contestuale dei dati personali possa comprendere e ricoprire i possibili utilizzi nell'ambito della vita *on-line* delle persone[134].

---

131 CODICE, Art. 4 - Definizioni, comma 1, lettera c): *"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato* ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*, 15 Dicembre 2011 (First Edition) p. 7

132 Identificatore che si riferisce, che può essere relativo o che può essere utilizzato per instaurare un collegamento tra il dato personale stesso e la persona (quindi ad esempio il codice fiscale, il numero di passaporto, o un numero di telefono oltre a nome, email ....); oppure contenere il valore di una caratteristica ugualmente distintiva (ad esempio un dato biometrico)

133 Sui dati oggetto di pseudonimizzaizone si rimanda al successivo paragrafo 3 – *L'anonimato e la protezione dei dati personali.*

134 Il caso è stato estratto da: WORLD ECONOMIC FORUM, *Rethinking Personal Data: Strengthening Trust* http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012), p. 34

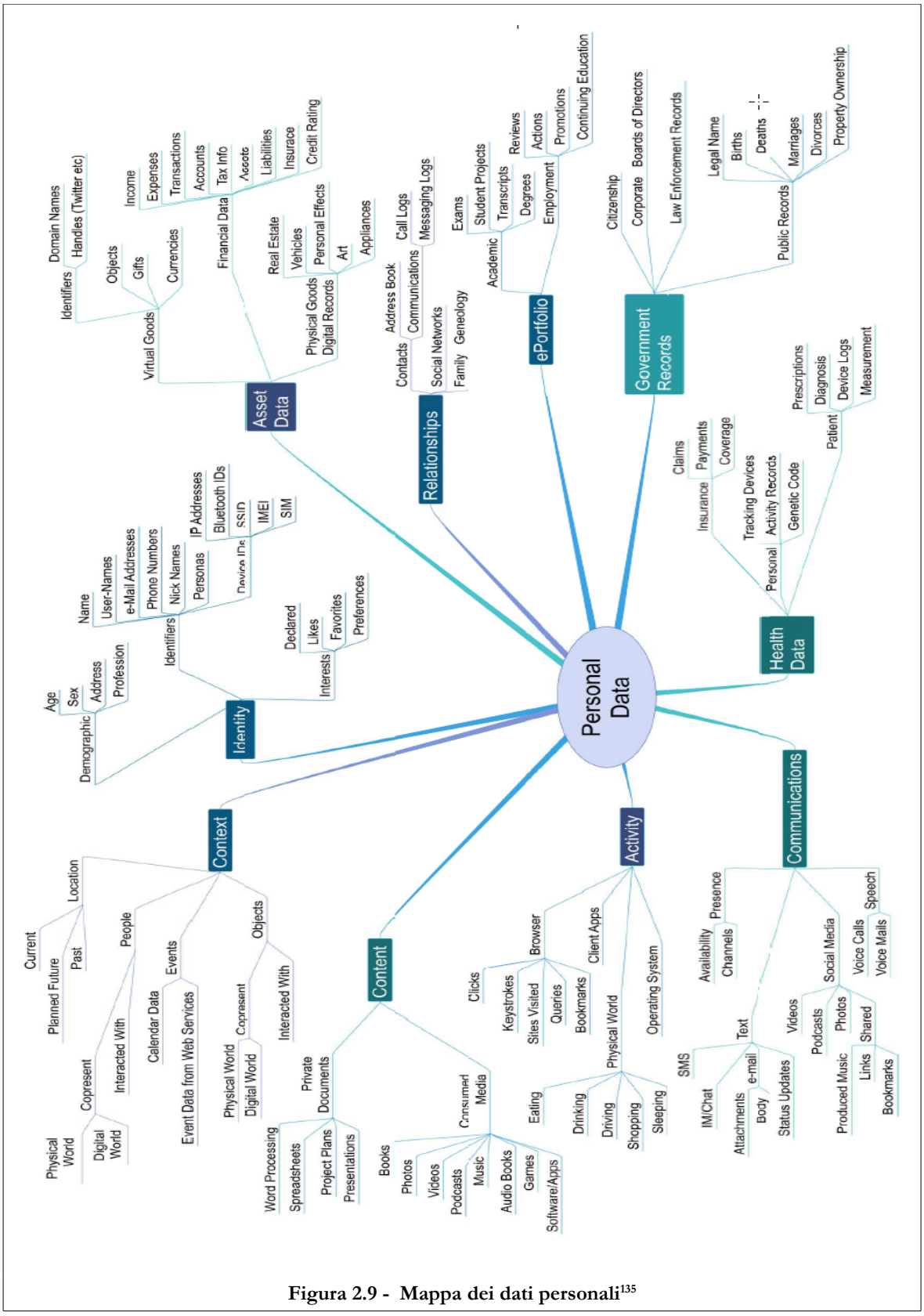


Figura 2.9 - Mappa dei dati personali[135]

[135] Fonte: Kaliya "Identity Woman" Hamlin and Personal Data Ecosystem Consortium.
Davis, Marc, Ron Martinez and Chris Kalaboukis. "*Rethinking Personal Information – Workshop Pre-read*" Invention Arts and World Economic Forum (2010)

2. La Privacy e la protezione dei dati personali.

Nel corso dell'elaborato ricorre quasi costantemente la congiunzione del termine *privacy* con l'espressione *protezione dei dati personali:* l'intento di questo accostamento non risponde ad una retorica di colore bensì al voler significare *Privacy per quel che attiene la protezione dei dati personali.*

Le due espressioni riflettono significati diversi: volendo semplificare, il primo include molto del secondo.

Dal 1890 quando ebbe inizio il dibattito sulla *Privacy* grazie al contributo *The right to be let alone*[136] pubblicato sulla rivista *Harvard Law Review* da Samuel D. Warren e Louis D. Brandeis, il concetto di *privacy* si è evoluto assai rapidamente (in particolare nell'ultima metà del secolo scorso) sia sotto il profilo della definizione della norma - della relativa verifica nella pratica giuridica e della configurazione dottrinale, sia per quel che attiene la progettazione e l'implementazione di soluzione operative tecnologiche e applicative. Tutto ciò, in breve tempo, ha portato la *privacy* a differenziarsi in plurime accezioni semantiche anche contraddittorie senza mai convergere in una definizione unica e comprensiva[137], ancor prima che se ne annunciasse una inarrestabile erosione o - al limite, la fine[138].

Probabilmente l'assenza di una tale definizione è riconducibile al fatto che la *Privacy* fin

---

136 Warren S., Brandeis L., *The Right to Privacy*, in Harvard Law Review, 1890, 4, p. 195, 205

137 Acquisti Alessandro, *Privacy,* Rivista di Politica Economica, V/VI, 319-368 (2005), p. 320

138 Eriksson J., *Privacy Is Dead: Long Live Surveillance Symmetry*, IEEE Internet Computing, Volume: 15, Issue: 1, Pages: 81 - 83, DOI: 10.1109/MIC.2011.18 (2011)

Preston Alex, The death of privacy - *Google knows what you're looking for. Facebook knows what you like. Sharing is the norm, and secrecy is out. But what is the psychological and cultural fallout from the end of privacy?* (2014)
Fonte: https://www.theguardian.com/world/2014/aug/03/internet-death-privacy-google-facebook-alex-preston

Hoanca B., *If Privacy Is Dead, What Can We Do Instead?*, IEEE Technology and Society Magazine, Volume: 35, Issue: 1, Pages: 29 - 37, DOI: 10.1109/MTS.2016.2518255 (2016), p. 29, 32

Lelio Simi, Pubblicità online, stiamo entrando nell'era della no-privacy su Internet - *Incrociare i dati sui comportamenti online e offline. Profilare tutto e rivenderlo, all'insaputa degli utenti. È la nuova frontiera dell'advertising di Facebook e Google* (11 Gennaio 2017)
http://www.pagina99.it/2017/01/11/pubblicita-online-web-advertising-no-tutela-privacy-su-internet-informativa/

Sull'argomento, inoltre, sono stati motivo di dibattito le posizioni di Scott McNealy, co-fondatore e CEO di SUN Microsystems, che nel 1999 durante un'intervista dichiarò: "*Consumer privacy issues are a red herring. You have zero privacy anyway. Get over it.*" http://www.pcworld.com/article/2941052/scott-mcnealy-on-privacy-you-still-dont-have-any.html

E di Mark Zuckerberg, fondatore e attuale CEO di Facebook, nel sostenere la *Privacy* non è più considerabile una norma, un valore sociale nella misura in cui riflette il mutato comportamento degli utenti a rilasciare e condividere le proprie informazioni sul social network. "*People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people," he said. "That social norm is just something that has evolved over time.*"
https://www.theguardian.com/technology/2010/jan/11/facebook-privacy.
Lo stesso Zuckerberg nella medesima intervista rilasciata a N. Bruno sul Corriere della sera dichiarò "*ormai finita l'era della riservatezza*". L'affermazione si riferiva volutamente alla riservatezza, sottolineando come Facebook, basato su una spiccata auto esposizione informativa, ha avuto grande successo. Il riferimento non era alla fine della protezione dei dati, e nemmeno della fine della *privacy* come tale, ma soltanto della fine del desiderio di riservatezza, del *right to be alone* nel quale si sostanzia la *privacy;* l'affermazione ebbe una risonanza assai ampia in parte anche distorta nel mutato e forzato significato.

dal suo nascere ha sempre rincorso l'affermarsi delle contingenti nuove tecnologie, dovendone bilanciare vantaggi e implicazioni d'uso più critiche, con l'obiettivo di rispondere ai diversi interrogativi che esse ponevano; tecnologie che a loro volta introducevano nuovi problemi sollecitandone nuove soluzioni, nuovi requisiti e quindi nuove concettualizzazioni.

Sul finire del 19° secolo la (nuova) tecnologia era rappresentata dalla fotografia istantanea veicolata dalle riviste di costume dell'epoca, rispetto alla quale (il diritto alla) la *privacy* nasceva per opporne le implicazioni intrusive verso il "*sacro recinto della vita privata e domestica*" – non solo connesse alla rilevazione ma alla loro diffusione, che minavano la tutela e la protezione dell'individuo nella misura in cui ne precludevano l'esercizio del diritto *ad essere lasciato da solo* (diritto di per se già componente la declinazione del diritto alla vita).

> *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" <...> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons <...>*
>
> **WARREN S., BRANDEIS L.,*The Right to Privacy,* 1890**

A distanza di poco più di mezzo secolo nel 1955, il *Right to be alone* viene posto al centro del noto saggio di William Faulkner: *On the privacy. The american dream: What happened to it,*[139] in cui in una visione essenzialmente letteraria l'autore sostanzia la *privacy* con la riservatezza.

Oggi le tecnologie sono i *Social Netwotk*, le *internet disruptive technologies* e i *Big Data analytics:* pervasive nella raccolta; intrusive nella misura in cui osservano per rilevazione, analisi, incrocio, collegamento; sorveglianti nella misura in cui profilano e deducono.

> *Modern life requires people to interact with big entities, and all these interactions require us to relinquish private information to entities we might not trust.*
>
> *The erosion of privacy is further exacerbated by the many information aggregators who are engaged in deliberate collection and dissemination of information.*
>
> *As the Internet is making the collection, distribution and use of information more available to anybody, privacy is steadily eroding.*
>
> *As privacy continues to be eroded and may even disappear, humankind will end up living in the virtual equivalent of a "small" village.*
>
> **HOANCA B., *If Privacy Is Dead, What Can We Do Instead?* (2016)[140]**

[139] Cfr in Harper's Magazine, 211, July 1955, disponibile alla risorsa http://harpers.org/archive/1955/07/on-privacy/

[140] HOANCA B., *If Privacy Is Dead, What Can We Do Instead?*, IEEE Technology and Society Magazine, Volume: 35, Issue: 1, Pages: 29 - 37, DOI: 10.1109/MTS.2016.2518255 (2016)

Applicate le dovute proporzioni, i due scenari condividono, un elemento cardine: entrambi - in forme rese diverse dai tempi e dalla tecnologia, sono contestualizzati sulla *circolazione* delle informazioni tra una pluralità di soggetti (oggi anche di oggetti). La *dinamicità* delle informazioni ha configurato il significato della *protezione dei dati personali* inteso come l'esercizio del diritto di ogni persona di controllare la *circolazione* delle proprie informazioni personali rispetto alle seguenti questioni iniziali che – ricalibrate dal contesto tecnologico, rimangono tutte valide e tutte aperte:

i. subordinare il trattamento al consenso, alla modifica o all'opposizione prevenitivamente rilasciati o riesaminati dalla persona in corso di trattamento (controllo);
ii. prevenire che lo stesso possa diventare la base unilaterale di scelte altrui che condizionano sia il rilascio delle informazioni sia la determinazione individuale a comporre e attuare le proprie scelte (autodeterminazione);
iii. mantenere la possibilità di perimetrare l'ambito e la profondità della propria personalità (o della sfera privata) accessibile a persone o sistemi (riservatezza);
iv. assicurare che l'immagine che il dato digitale veicola di una persona (il profilo) si mantenga coerente e allineata con quella reale senza falsarla, distorcerla o precluderne revisioni (personalità);

e rispetto alle quali il controllo della circolazione dei dati personali è stato modulato, per l'appunto, sull'evolvere delle modalità stesse con cui le informazioni acquisivano sempre maggiore dinamicità passando dal coinvolgere pochi e privilegiati soggetti[141] all'intera

[141] Fintanto che la gestione elettronica delle informazioni (anche personali) si è mantenuta finalizzata all'essere strumento di calcolo prerogativa di pochi centri di ricerca o organismi militari, centralizzata e non soggetta ad alcuno scambio di dati in rete se non quello di di collegamento e visualizzazione tra il mainframe e i propri terminali, il controllo ne risultava semplificato tanto quanto lo stesso trattamento (limitato all'immissione, elaborazione e archiviazione), immediato per la tempestività di verifiche puntuali, e sostanzialmente subordinato all'autorizzazione di un'unica autorità di controllo.

La diffusione dei personal computer, la capillarità dell'elaborazione e quindi di un trattamento esteso nelle caratteristiche, cambiava notevolmente la prospettiva della protezione dei dati personali rendendola più flessibile nella misura in cui affiancava, per un verso, l'interessato al responsabile del trattamento e all'Autorità di Controllo, distribuendone quindi i poteri di controllo e intervento; e, per un altro, controbilanciando all'assenza di autorizzazioni per i trattamenti rispondenti a legittimi interessi e privi di rischi per la persona, l'introduzione di limiti rigorosi per i trattamenti più critici e pericolosi (attinenti per esempio i dati sensibili), di garanzie della correttezza e della sicurezza del trattamento; la presenza di una Autorità di Controllo imparziale con il compito di sovrintendere alla protezione dei dati, ma soprattutto l'introduzione di diritti di controllo dell'interessato delineando quindi la precisa volontà di inquadrare il tema alla protezione dei dati personali nel diritto della personalità e dell'autodeterminazione individuale.

Questo orientamento emergeva, intorno agli anni '80, nelle prime discipline sulla protezione dei dati personali adottate in alcuni paesi europei come Francia, Germania e Regno Unito, recepito dalla Direttiva 95/46/CE - *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,* attuata in Italia con l'emanazione della legge 31 Dicembre 1996 n.675 in un ambito in cui la *circolazione* dei dati personali non oltrepassava i confini delle banche dati e dell'elaborazione elettronica ed automatizzata delle informazioni. Successivamente, con il Decreto Legislativo 30 giugno 2003, n. 196 - *Codice in materia di protezione dei dati personali* l'Italia evolveva e ripensava totalmente il recepimento della Direttiva europea con una lungimiranza che recuperava un certo ritardo iniziale, rispondendo all'ormai affermazione di Internet e ad una *circolazione* delle informazioni interconnessa, collegata, integrata, strutturata e accessibile; condivisa e riutilizzabile negli utilizzi e nelle finalità.

collettività, sino a divenire una *questione di interesse pubblico e sociale* nella misura in cui la protezione dei dati personali non risponde più solo alla tutela della persona ma si estende alla tutela dell'intera società alla quale essa appartiene[142]; una società che vive in una dimensione in cui il trattamento digitalizzato è la struttura portante di ogni relazione interpersonale, in cui la distinzione tra realtà fisica e virtuale è sparita così come quel concetto di sfera privata che consentiva alla persona di esercitare il diritto ad *essere lasciata (da) sola.*

[142] CODICE, considerando 4) *Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità* <...>

2.1. I MOLTEPLICI SIGNIFICATI DELLA PRIVACY.

Trattare la *privacy* è un termine polisenso che incrocia ambiguità semantiche e contraddizioni, in letteratura non si rileva una unica e comprensiva definizione che soddisfi le molteplici funzionalità e interpretazioni; inoltre sull'argomento, il dibattito è stato, e tuttora persiste ancorato ad interessi contrapposti, ad una ambiguità della definizione, e ad una serie di reazioni individuali e collettive variabili dal rifiuto e disinteresse, alla pragmaticità di attenzionare la questione in contingenza di specifiche necessità o convenienze, al difendere la protezione dei dati personali incondizionatamente, ritenendola un diritto (fondamentale) esercitabile dalla persona e un dovere per gli altri soggetti rispettarlo[143]; per alcuni soggetti può essere considerato un valore positivo, per altri neutrale; altri ancora - ed è la situazione maggiormente ricorrente, mutare atteggiamento a seconda di come gli sviluppi tecnologici e informativi hanno mutato i confini tra la c.d. sfera pubblica e quella privata.

Tradotto letteralmente al termine *privacy* corrisponde quello della privatezza o della riservatezza e tradizionalmente il significato riflette e veicola una esigenza di attenzione, di difesa, di protezione e di salvaguardia da possibili interferenze dirette verso la propria sfera individuale.

La differenziazione semantica della *privacy* è stata sollecitata dal rivoluzionarsi delle tecnologie della comunicazione e dell'informazione, dalla loro pervasiva diffusione con costi sempre minori e sostenibili, che per un verso hanno catalizzato il sorgere di ulteriori tecnologie intrusive – modificando prima e dilatando poi il perimetro della sfera privata verso quella pubblica, e per un altro – ciclicamente, introducendo nuove contromisure di difesa.

Alessandro Acquisti - docente di economia pubblica alla Carnegie Mellon University (Pittsburgh, Pennsylvania, USA) ed esperto di economia della *privacy,* nel contributo *Privacy* pubblicato durante il 2005 nella Rivista di Politica Economica illustra le interpretazioni assunte nel tempo dal concetto di *privacy:* percepita come controllo e protezione di un'ampia sfera privata, intesa come personale e intima; oppure come spazio fisico, mentale o digitale; o ancora come ambito individuale risultante di dati e informazioni personali, in cui il controllo può essere esercitato in senso informativo, decisionale, o di processo; strumentale alla protezione della dignità umana[144], un diritto inalienabile; ritenuta affermazione di libertà o forma di solitudine; supporto per un benessere, una rassicurazione psicologica della persona;

[143] ACQUISTI ALESSANDRO, *Privacy,* Rivista di Politica Economica, V/VI, (2005) p. 320

[144] Su tale accezione si rimanda alla posizione di Luciano Floridi *On Human Dignity as a Foundation for the Right to Privacy*, Philos. Technol. DOI 10.1007/s13347-016-0220-8, Springer Science+Business Media Dordrecht 2016

o al limite espressiva di una copertura verso l'ipocrisia, l'inganno, il rifiuto delle proprie responsabilità.

Da qualunque prospettiva si osservi la concettualizzazione della *privacy,* la convergenza di interessi contrapposti risulta costante ed evidente e riflette un continuo intreccio tra lo spazio privato e pubblico di una persona: in ambito relazionale all'esigenza di *privacy* e all'interesse di protezione delle proprie informazioni si contrappone il desiderio di comunicare, di condividere, di esibirsi; all'iniziale interesse volto al controllo e trattenimento dei propri dati personali si oppone l'interesse alla divulgazione spinta da sconti o compensazioni monetarie; per richiamare il caso di studio illustrato al paragrafo 1.2. - *La centralità dell'utente nel disclosure dei dati personali* l'informazione che un utente rivela ad un servizio può essere utilizzata per rendere la navigazione più efficiente e accessibile, ma anche per studiare e analizzare le attitudini del consumatore, prevederne il comportamento e anticipare, per finalità di guadagno, la propensione all'acquisto di certi prodotti.

Di seguito sono elencate le interpretazioni semantiche della *privacy* più ricorrenti e pratiche, connesse alla disamina tanto delle criticità e dei rischi occorrenti nella gestione dei dati personali, tanto delle relative contromisure applicative. Il significato della *privacy* può attenere:

1. la *riservatezza* intesa come mantenimento della segretezza delle informazioni, di per se è un concetto legato alla staticità dei dati, condivisi (in quanto segreti) con un ristrettissimo gruppo di persone. In tal senso è da considerarsi associata ad una sorta di *possesso* esercitabile sulle proprie informazione, volta a tutelare la sfera *individuale* da interferenze o indiscrezioni altrui. Rispetto all'evolversi di questo significato (cfr successivo punto) è significativo (per quanto lievemente anacronistico) rappresentare la riservatezza utilizzando il trinomio (persona, informazione, segretezza) introdotto e utilizzato da Stefano Rodotà[145] per declinarne il diritto (alla riservatezza);
2. la *protezione* inteso come controllo sulla circolazione dei propri dati personali da considerare quindi, nella loro dinamicità: risulta rappresentativa la rimodulazione del precedente trinomio in (persona, informazione, *circolazione*, segretezza). L'esercizio del controllo può essere implementato con il ricorso a tecniche più propriamente rientranti nelle contromisure di sicurezza: ad esempio l'oscuramento dei dati identificativi mediante pseudonimizzazione e cifratura; oppure mediante la

[145]RODOTÀ S., *Privacy e costruzione della sfera privata*, in Id., "Tecnologie e diritti", Bologna, Il Mulino, 1995.

configurazione di diritti, responsabilità e permessi volti specificatamente a controllarne e monitorarne l'utilizzo: ad esempio la definizione e il rilascio del consenso in relazione allo specifico utilizzo e scopo; i permessi di accesso, di rettifica, di cancellazione, di limitazione, di sospensione di utilizzo sono tutte tipologie di politiche volte al controllo d'uso dei dati personali. Con riferimento al diritto alla protezione dei dati personali, questo disciplina che le proprie in informazioni siano sempre trattate nel pieno rispetto dei presupposti e dei limiti definiti dalla legge;

3. la *trasparenza,* si aggancia al precedente punto per due ragioni, e solo apparentemente risulta opporlo, significando – quindi, un ottimo esempio di convergenza di interessi diversi. Per il titolare dei dati personali (il soggetto interessato) la trasparenza è il presupposto per l'esercizio del consenso informato e per l'implementazione consapevole di tutti i permessi d'uso; per le altre parti coinvolte nella gestione dei dati personali è il presupposto di diffusione delle informazioni e la conseguente possibile libertà di rilevarle ed elaborarle, per sviluppare le proprie conoscenze utilizzando dati concernenti altri soggetti. La trasparenza inoltre è premessa necessaria per
4. l'*autodeterminazione,* anch'essa una forma di controllo sui propri dati che attiene la prerogativa del soggetto interessato di determinare e attuare scelte consapevoli sull'uso e il trattamento dei propri dati;
5. il mantenimento dell'*identità personale:* ovvero la corretta rappresentazione della persona durante l'intero ciclo di gestione delle informazioni;
6. l'*anonimato,* processo che interrompe l'associazione (diretta o indiretta) con il soggetto interessato, puntando ad una de-identificazione irreversibile;
7. il *nascondere* l'informazione – tale da essere omessa o errata, che per un verso oppone un altro diritto rilevante - ovvero quello di non privare altri della conoscenza e dell'accesso all'informazione[146]; e per un altro la qualità dell'informazione intesa nelle sue caratteristiche di accuratezza, esattezza, appropriatezza;
8. la *qualità dei dati,* nella misura in cui la *privacy* presuppone e supporta l'implementazione e il mantenimento dei requisiti di *esattezza* e *correttezza, pertinenza, accuratezza, completezza, non-ridondanza (minimizzazione), validità temporale; coerenza e appropriatezza.*
9. la *sicurezza,* nella misura in cui la *privacy* presuppone e supporta: *i)* la valutazione dei

[146] ACQUISTI ALESSANDRO, *Privacy,* Rivista di Politica Economica, V/VI, (2005) p. 319-368
POSNER R.A., *An Economic Theory of Privacy,* Regulation, (1978), p. 19-26,.
The Economics of Privacy, American Economic Review, vol. 71, n. 2, 1981, p. 405-09.

rischi associati e derivabili dalla gestione dei dati personali, richiedendo una definizione proattiva delle contromisure fin dalla progettazione del trattamento (in termini di mezzi e finalità del trattamento), secondo la metodologia del *privacy by design/default; ii)* l'incrocio dei requisiti di riservatezza, integrità e disponibilità, la resilienza e la capacità di *disaster recovery* dei sistemi;

10. infine alcune delle precedenti interpretazioni declinabili come diritto, quindi: diritto alla riservatezza, alla protezione dei dati personali, alla trasparenza e all'accesso in entrata ed in uscita all'informazione; all'autodeterminazione, all'anonimato, alla liceità e alla sicurezza del trattamento.

2.2. La modellazione della Privacy.

La seguente figura 2.10 sintetizza graficamente le considerazioni illustrate al precedente paragrafo. I riquadri più chiari indicano caratteristiche della *privacy* di frontiera, oggetto di studi recenti e tutt'ora in fase di sviluppo; alcune di queste - legate al concetto di proprietà del dato personale, alla pluralità di soggetti interessati, al valore economico dei dati personali e della privacy, saranno trattate nei capitoli 4 – *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.* e 5 - *Progettazione di un modello di supporto a politiche di privacy user e data centric.*

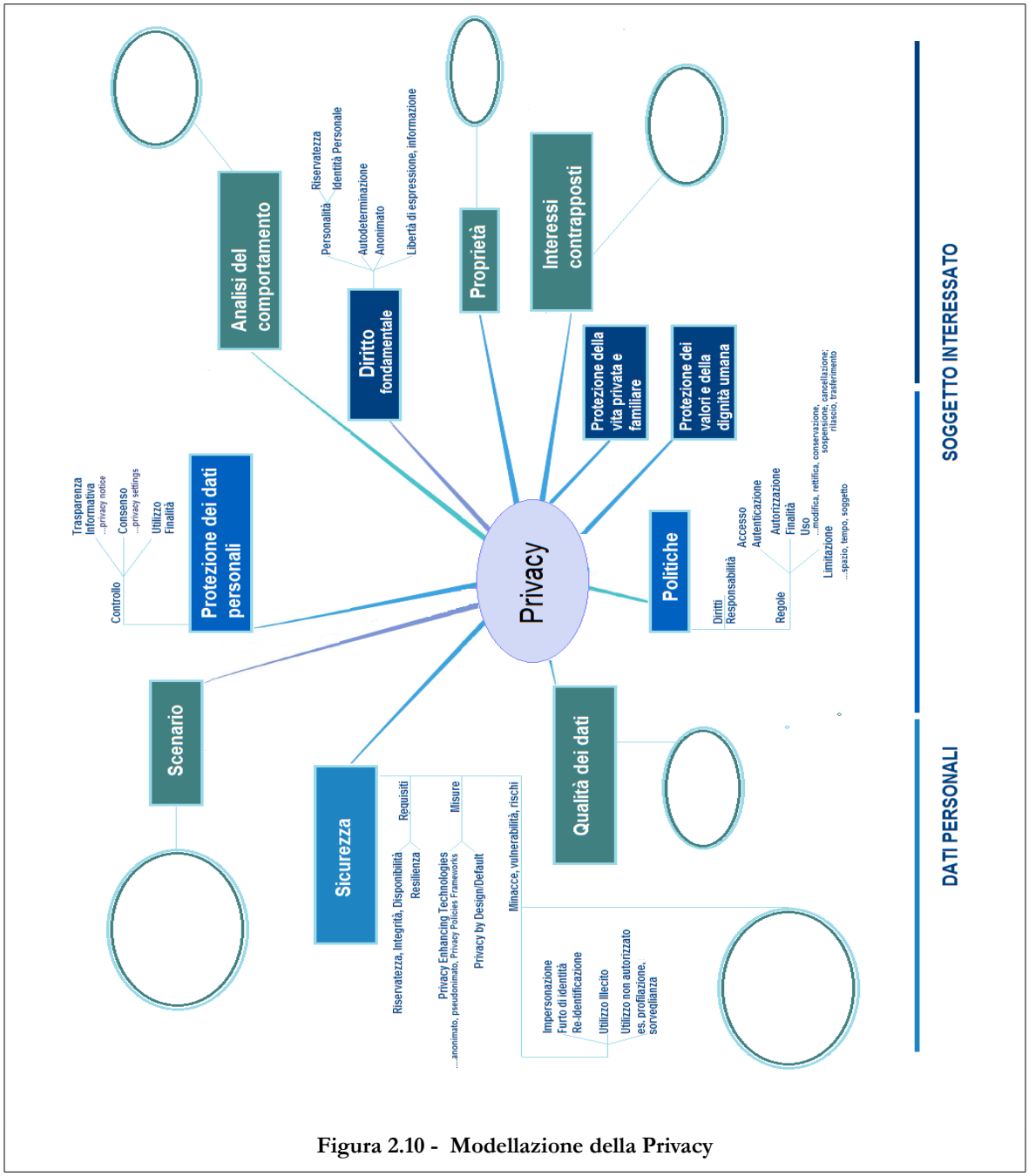


Figura 2.10 - Modellazione della Privacy

2.3. LA PROTEZIONE DEI DATI PERSONALI: CRITICITÀ E RISCHI CONNESSI ALLA GESTIONE DEL DATO.

Le *Internet disruptive technologies, Big Data* e *IoT, Social Media* nonchè i costi di interconnessione e di *storage* sempre minori hanno reso più efficiente la produzione massiva, lo studio e l'analisi dei dati personali, consolidando e affermando tradizionali forme di rischio e introducendone di nuove, che si configurano come elemento contrapposto alle nuove tecnologie che migliorano e aumentano la vita delle persone per qualità, efficienza dei servizi e dei prodotti offerti.

Più le persone e le aziende utilizzano le nuove tecnologie, meno costosa e più veloce diventa la produzione di dati personali; più i dati personali vengono prodotti e rilasciati, più aumentano i rischi: ogni attività in rete lascia tracce che monitorate, collegate e riutilizzate per scopi differenti possono essere associate alle persone e ricostruirne la vita quotidiana[147], con scarso o nullo controllo - a *disclosure* effettuato, da parte dell'interessato che raramente è in grado di valutare i rischi implicati dalla rilevazione e dalla divulgazione dei propri dati personali, contezza che generalmente sorge solo a-posteriori di un evento dannoso in contingenza delle relative conseguenze attinenti la propria identità, il profilo, le credenziali, la propria immagine, la propria reputazione, il proprio denaro.

Le minacce, i rischi, i pericoli e le violazioni[148] connesse al trattamento dei dati personali possono essere distinte in due tipologie:

i. la prima comprende quelle tipiche della sicurezza informatica attinenti quindi violazione dei requisiti di confidenzialità, integrità, autenticità, disponibilità[149] ai quali corrispondono le relative contromisure rientranti nella sicurezza logico/applicativa/sistemistica (protocolli sicuri, infrastrutture di crittografia, antivirus, personal firewall, Virtual Private Network, networking monitoring, contrasto del proof-of-concept…); in questo insieme le informazioni personali sono innanzitutto

[147] A titolo di esempio si richiamano le seguenti tipologie di informazioni che diventano dati personali per il tramite della relazione di attribuzione e idenficabilità tra le persona e le sue credenziali di accesso (dati di login, numero di telefono, immagine personale), piuttosto che con il device *posseduto* o indossato: ogni utilizzo di servizi Web e Social tracciato da login di accesso, da cookies analitici e di profilazione, da motori di ricerca, da log applicativi di Apps di messaggistica, da ogni aggiornamento di contenuti in blog, post, condivisioni, upload, hashtag...; ogni utilizzo di servizi *mobile e wireless* tracciato da geolocalizzazione GPS, RFID, NFC, Bluetooth; ma anche flussi di transazioni finanziarie, carte di credito, bollette; o ancora dati rilevati da oggetti *IoT* di *quantified self, wearable computing* o *domotici* che rilevano, misurano, registrano e trasmettono abitudini, stilisi vita, movimento delle persone.

[148] In questo passaggio si fa riferimento al paradigma (minaccia, rischio, pericolo; vulnerabilità) dove per rischio si intende l'eventualità di un pericolo nel presupposto dell'esistenza di minacce verso le quali un sistema di gestione delle informazioni (nel caso specifico il trattamento) presenta della vulnerabilità. Cfr *Innovazione e tecnologie Ingormatiche*, Management, Edito da Il sole24ore, Università Boccono Editore, La Repubblica, pag. 200-201.

[149] In argomento si rimanda alla seguente fonte: D'ACQUISTO G., NALDI M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017) pag. 191 - 201

informazioni, processate in quanto tali indipendentemente dall'attribuzione ad una specifica persona;

Industry	Total	Small	Large	Unknown
Accommodation	362	140	79	143
Administrative	44	6	3	35
Agriculture	4	1	0	3
Construction	9	0	4	5
Educational	254	16	29	209
Entertainment	2,707	18	1	2,688
Finance	1,368	29	131	1,208
Healthcare	166	21	25	120
Information	1,028	18	38	972
Management	1	0	1	0
Manufacturing	171	7	61	103
Mining	11	1	7	3
Other Services	17	5	3	9
Professional	916	24	9	883
Public	47,237	6	46,973	258
Real Estate	11	3	4	4
Retail	370	109	23	238
Trade	15	3	7	5
Transportation	31	1	6	24
Utilities	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Figura 2.11 – Report Verizon 2016: numero di incidenti di sicurezza nell'anno 2015 per settore coinvolto e dimensione di azienda[150].

ii. nella seconda tipologia rientrano rischi e violazioni proprie della *privacy* configurabili sulla intrinseca associazione di riconducibilità (diretta o indiretta) delle informazioni con il soggetto interessato[151] e come tali portanti un forte impatto per la persona, incidendo sui diritti e sulle libertà fondamentali; rientrano quindi, tra i rischi e gli attacchi per la *privacy:* il furto di identità e di dati personali[152] (credenziali, dati identificativi, dati di profilo, carte di credito), l'impersonazione, la sorveglianza e la profilazione non autorizzata, la re-identificazione di dati anonimi[153], qualsiasi utilizzo o

[150] Fonte: Presentazione *CyberSecurity&Privacy – L'assicurazione del rischio sui dati,* avv.to Rocco Panetta Atti: PrivacyDay Forum organizzato da FederPrivacy e tenutosi a Roma il 13 Ottobre 2016.

[151] Si richiama in tal senso la definizione di dato personale contenuta nel GDPR, art. 4 *Definizioni* comma 1) *«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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;*

[152] I report annuali rilasciati dal CLUSIT (Associazione italiana per la Sicurezza Informatica) per gli anni 2015 e 2016, documentano ed evidenziano che per entrambe le annualità tra i 10 attacchi alla sicurezza delle informazioni 3 di questi concernono il furto di dati identificativi, carte di credito e azioni di spionaggio sulle attività on-line degli utenti. In argomento per i dettagli si rimanda alla fonte:
CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, *Rapporto CLUSIT 2015* e *2016 sulla sicurezza ICT in Italia*, disponibile su: https://www.clusit.it/download/index.htm

[153] In argomento si rimanda al successivo capitolo 3 - *Privacy e Protezione dei Dati personali: le contromisure,* paragrafo 2.1. - *L'anonimato e la protezione dei dati personali*. e alla seguente fonte: D'ACQUISTO G., NALDI M., *Big Data e Privacy by Design*

trattamento illecito e non autorizzato delle informazioni personali; ma anche tipologie di criticità meno tangibili e più contestuali connesse alla quantità e alla tipologia dei dati divulgati, al media che li veicola al contenitore che li pubblica, alla pluralità dei soggetti che li condividono e li utilizzano.

Attacchi alla *privacy* e alla protezione dei dati personali – ai quali oppone il complesso di contromisure *PETs Privacy Enhancing Technologies*[154]*,* che catturano l'attenzione degli utenti e che impattano la percezione del pericolo e del danno, coinvolgono diversi settori per tipologia e dimensione (cfr precedente figura 2.11) e sono sempre più frequentemente pubblicati sia dai media del settore che da quelli più divulgativi; si riportano - a titolo di esempio, alcuni dei casi più recenti:

- ✔ Cybersecurity, anche le commodity nel mirino degli hacker - *Report Idc: il 60% delle multinazionali europee subirà attacchi finalizzati all'interruzione di produzione e distribuzione di beni e servizi. I dati restano comunque il bersaglio preferito, tanto che l'85% dei consumatori abbandonerà un servizio commerciale in seguito a una violazione*[155] (Fonte: Cor.Com.it, 2017);
- ✔ Hacker in azione su Whatsapp e Telegram: allarme foto ruba-dati – *Cybersecurity, La scoperta dei ricercatori di Check Point Software Technologies. Basta aprire dall'applicazione web una foto apparentemente innocua per consegnare scatti, video e informazioni ai criminali informatici*[156] (Fonte: Cor.Com.it, 2017);
- ✔ Privacy, Oracle denuncia Google alla Ue: "Crea super-profili" – *Il caso, Nel mirino le modalità di raccolta dati che mettono insieme sia quelli sulla navigazione sia quelli delle ricerche: "Così può offrire pubblicità mirate in modi che gli altri concorrenti non possono". La risposta di BigG: "Accuse prive di sostanza, il nostro sistema è totalmente opt-in"* [157](Fonte: Cor.Com.it, 2017);

Anonimizzazione Pseudonimizzazione Sicurezza, G. Giappichelli Editore (2017) pag. 187-191 in cui gli autori elencano esempi molto significativi di de-anonimizzazione in contesti di geolocalizzazione, mobilità, proof-of-concept di database.

[154] Le *PETs* possono considerarsi misure di sicurezza logico/applicativa specificatamente applicabili alle informazoni di carattere personale. Esse comprendono 3 macro categorie di misure: l'anonimizzazione, la pseudoanonimizzazione e i frameworks di privacy policies. Le prime due misure – per la stretta attinenza alla relazione di identificabilità dato-persona, saranno trattate a chiusura del presente capitolo. Ai frameworks di *privacy policies* è dedicato il capitolo 3 - *Privacy e Protezione dei Dati personali: le contromisure.*

[155] In argomento la fonte è disponibile su: http://www.corrierecomunicazioni.it/digital/46738_cybersecurity-anche-le-commodity-nel-mirino-degli-hacker.htm, 11 Aprile 2017 di Andrea Frollà.

[156] In argomento la fonte è disponibile su: http://www.corrierecomunicazioni.it/digital/46356_hacker-in-azione-su-whatsapp-e-telegram-allarme-foto-ruba-dati.htm, 16 Marzo 2017 di Andrea Frollà.

[157] In argomento la fonte è disponibile su: http://www.corrierecomunicazioni.it/digital/45524_privacy-oracle-denuncia-google-alla-ue-crea-super-profili.htm, 25 Gennaio 2017 di F.Me.

- ✔ L'infezione di Eye Pyramid: il malware che spiava i potenti italiani - *L'anello debole della catena è sempre l'utente, che cliccando sull'allegato malevolo ha permesso l'installazione del software spia. Come funziona la botnet dei fratelli Occhionero*[158](Fonte: Repubblica.it, 2017);
- ✔ Attacco hacker a Yahoo: "Rubate chiavi d'accesso a mezzo miliardo di utenti - *La conferma dall'azienda di Sunnyvale che aggiunge: hacker al servizio di uno Stato straniero. A rischio ora la cessione delle attività chiave della società internet*[159] (Fonte: Repubblica.it, 2016)
- ✔ Truffe on-line in italia: 40.000 casi nel 2016 di cui il 40% delle vittime sono over 65; 3000 casi tra minacce, ingiurie e diffamazione in rete, 100 casi di stalking on-line oltre 20 nel 2017; falso profilo Instagram della Polizia Postale Ialiana[160] (Fonte: Polizia Postale Italiana, 2017)

Ma è il Web, in particolare le reti sociali e le apps di messaggistica nonché le tante chat a cui è possibile partecipare, l'ambiente *on-line* in cui si attuano e consumano con maggiore intensità e frequenza le violazioni sui dati personali: *Facebook*, *Instagram*, *Twitter, Google+; WhatsApp e Telegram*. Piattaforme divenute molto popolari e che presuppongono il necessario rilascio di dati identificativi (nome e cognome, immagine) nella inizializzazione e nella configurazione del profilo[161]. Si chiamano reti sociali, proprio perché servono a far rete e a socializzare, mostrano ed espongono l'utente in ogni situazione, comunicano chi l'utente *è,* il suo quotidiano, i suoi viaggi, i suoi amici, gli acquisiti effettuati e pensati, le informazioni personali quelle che, spesso si tenderebbe a tenere riservate.

Il proprio profilo - nativamente *nonimo*[162]*,* diventa una identità pubblica liberamente circolante e accessibile a tutti, così come il proprio pensiero che diventa interpretabile da chiunque, le proprie foto e i propri video che diventano istantaneamente ri-utilizzabili. Gli utenti con meno di 30 anni utilizzano quotidianamente 3-5 social network diversi, alimentando di default la replica dei propri dati personali senza poter materialmente intercettarne o rimuoverne il contenuto a rilascio avvenuto. Aspetto non secondario, l'assenza - nei social media[163], di un filtro di selettività in ingresso tanto sugli utenti tanto sulla pubblicazione delle

158 In argomento la fonte è disponibile su: http://www.repubblica.it/tecnologia/2017/01/11/news/l_infezione_di_eye_pyramid_il_malware_che_spiava_i_potenti_italiani-155810678/, 11 Gennaio 2017 di Simone Cosimi.

159 In argomento la fonte è disponibile su: http://www.repubblica.it/tecnologia/sicurezza/2016/09/22/news/attacco_hacker_a_yahoo_rubate_chiavi_d_accesso_a_200_milioni_di_utenti_-148310314/, 22 Settembre 2016

160 In argomento la fonte è disponibile su: https://www.commissariatodips.it/notizie.html

161 Facebook Inc, che nasce nel 2004, in particolare è stato il primo social media a richiedere come obbligatori dati identificativi dell'utente nella configurazione del profilo. Lo precedettoro altri social media ad esempio *MySpace.com* (fondato da Tom Anderson e Chris DeWolfe nel 2003) che non prevedevano questa caratteristica.

162 Nel senso di contrario del termine anonimo.

163 In cui - aspetto non residuale, il numero di *followers* o di amici, rappresentano l'unità di misura dell'importanza di una

informazioni, condivise indiscriminatamente nella rete dei contatti, favorisce un riutilizzo delle informazioni non conforme alle aspettative dell'utente.

In questo contesto le violazioni più frequenti sui dati personali sono legate al furto di informazioni e di credenziali, all'impersonazione e alle false identità che si propongono e si avvicinano per sottrarre fiducia, relazioni, sentimenti e (spesso) denaro; alla distorsione della propria identità personale, allo scredito della propria reputazione e della propria immagine; alla diffamazione e al disonore che ne derivano.

Questo scenario risulta di per se e in linea di principio distorto, ma ovviamente acquisisce la dimensione della pericolosità quando dall'altra parte della rete operano soggetti motivati da obiettivi di guadagno più o meno facili o lecito utilizzando asimmetricamente le informazioni personali altrui; o al limite persone disturbate o persone che puntano alla truffa o al ricatto.

Nel capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche* verranno illustrati e approfonditi gli scenari ed alcuni esempi di nuove tipologie di rischio in contesti di forte inferenza informativa: *IoT*, *Big Data* e *Data Mining, Realtà Aumentat* e *App* per *smart devices*. In questo frangente interessa focalizzare la riflessione sulla principale ragione di vulnerabilità che presuppone alle violazioni descritte:

- ✔ essa risiede nella natura intrinseca di *data-accretion* del media digitale (condivisibile, moltiplicabile e riutilizzabile infinitamente, e – in pratica, a costo *zero)* e nel fatto che il volume di dati circolante è divulgato, rilasciato, condiviso e reso pubblico per volontà degli stessi utenti; una volontà fortemente direzionata (se non costretta) dalla obbligatorietà di rilasciare i propri dati personali identificativi per poter accedere e fruire ai servizi proposti.

La spinta motivazionale (o il vincolo) a divulgare i propri dati porta a sottovalutare come e quanto il media digitale possa rivelarsi pericoloso: la pubblicazione, il *disclosure* e la condivisione in rete di una foto, di un commento, di un pensiero, di un documento, di una identità on-line, ne amplifica dinamicamente l'immaterialità rendendolo duplicabile e ri-utilizzabile infinite volte, coincidendo con una perdita di controllo sulla proprie informazioni.

Questa perdita di controllo diventa totale quando le informazioni personali volontariamente rilasciate dall'utente nei limiti di una specifica finalità di utilizzo sono agganciate ad altre, sempre riferibili all'utente ma disponibili non per sua volontà, divulgati

persona ed il segnale di successo personale e di affermazione sociale.

non per sua autorizzazione, quindi collezionati e riutilizzati a sua totale insaputa. Questo, per esempio è il semplice caso di foto di gruppo pubblicate sui social media; oppure un esempio più raffinato è quello in cui l'utente diventa un non-utente[164] nel contesto delle rilevazioni fotografiche o video effettuate da altre persone con *smart glasses* la cui funzione è quella di aumentare il contesto ripreso associando ad un luogo le coordinate di geolocalizzazione o la storia, così come ad un volto il nome, il cognome, la data di nascita, gli amici *scaricati* da Facebook, piuttosto che la professione da Linkedin.

Il problema della *privacy* e della protezione personale, quindi per quanto precede, non è affatto nuovo; rinnovata è l'abilità di raccogliere, manipolare, studiare e reagire ad un volume di dati praticamente in tempo reale – senza il controllo della persona il cui intervento, in linea di massima, è limitato e circoscritto alla produzione e al rilascio delle proprie informazioni; senza che la persona possa quindi seguire e governare le proprie informazioni durante la loro circolazione e il loro riutilizzo. La *privacy* negli o*n line social network* può ritenersi un grande esperimento di regolazione del *disclosure* di dati personali di cui nessuno dei partecipanti conosce l'esito finale.

Criticità, rischi e violazioni che ne conseguono concorrono, tra l'alto a configurare ed alimentare la tensione di criticità che grava sul trattamento dei dati personali e che contrappone alla sempre maggiore spinta sulla persona ad esporre e condividere i propri dati *on-line* un calo di fiducia, diffidenza e preoccupazione; una scarsa consapevolezza, un approccio alla questione reattivo (a violazione avvenuta) piuttosto che proattivo, una residuale partecipazione dell'utente favorito anche da una scarsa espressività e trasparenza delle politiche di controllo e che innescano quindi dubbio e sospetto, perdita di controllo e percezione di pericolo per le proprie informazioni che aumenta proporzionalmente quanto tale controllo tende a passare ad essere unilateralmente esercitato da chi raccoglie e sfrutta i dati personali soprattutto per scopi e utilizzi secondari e diversi da quelli acconsentiti inizialmente e attesi dall'utente.

[164] Nello specifico, questo argomento sarà oggeto di approfondimento nel capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche*

2.4. LA PROTEZIONE DEI DATI PERSONALI: LA CENTRALITÀ DELL'UTENTE TRA *STATUS QUO*, TRASPARENZA E CONTROLLO.

Quali sono le spinte motivazionali per la persona a proteggere (o non proteggere) i propri dati personali? Per gli utenti la *privacy* è una questione importante?

Gli attori coinvolti nella gestione delle informazioni personali (soggetti interessati, organizzazioni, istituzioni e organismi di regolazione, titolari e responsabili) condividono, seppur in forme e prospettive diverse, preoccupazioni su come i dati personali sono gestiti e protetti, trasferiti da una azienda e da un titolare all'altro.

Tra gli utenti cresce la sfiducia, il dubbio, la diffidenza nel modo in cui i titolari del trattamento dei dati personali (*stakeholders,* organizzazioni aziendali e governi) usano i loro dati; al contempo nelle organizzazioni cresce la tensione connessa alla propria effettiva capacità di proteggere i dati personali trattati senza accrescere le preoccupazioni degli utenti, mantenendone la fiducia ed evitare possibili decrementi di crescita e di profitto, nonché poterli efficacemente sfruttarli in concorrenza con i propri *competitors;* le istituzioni giuridiche (comunitarie e non) reagiscono nel definire contromisure regolatorie che possano conciliare in maniera efficace la tutela della protezione delle persone e dei dati personali senza paralizzare l'evoluzione di una società sempre più basata sulla circolazione delle informazioni digitali[165].

Limitando la disamina ai soggetti interessati è possibile individuare tre tipologie di utenti[166]: i *pragmatici* – disponibili a rivelare i propri dati in relazione alle contingenti convenienze; i *fondamentalisti* che credono nella *privacy* in quanto tale e in quanto diritto che gli altri soggetti devono rispettare; e i *rilassati* che non sembrano avvertire particolari preoccupazioni per le criticità e i rischi del trattamento dei propri dati. Le prime due categorie sono le più comuni, *pragmatici* e *rilassati,* inoltre, mostrano scarso interesse per l'utilizzo delle tecnologie di protezione.

Su questo tema si ritiene utile riportare gli esiti delle indagini statistiche tematiche svolte dall'Eurobarometro per conto della Commissione Europea[167], condotte nel Marzo del 2016 su

---

[165] In argomento, per un maggior dettaglio, si rimanda alla seguente risorsa del WORLD ECONOMIC FORUM, *Rethinking Personal Data: Strengthening Trust,* http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012) pag. 10-12

[166] ACQUISTI ALESSANDRO, *Privacy and Security of Personal Information: Technological Solutions and Economic Incentives*, In J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 165-178 (2004)

ACQUISTI ALESSANDRO, TAYLOR CURTIS R., WAGMAN LIAD, *The Economics of Privacy,* Journal of Economic Literature, forthcoming (2015).

Alessandro Acquisti ricostruisce sull'argomento le posizioni e le fonti più affermate disponibili nella recente letteratura sull'economia comportamentale della privacy: Alan Westin 1991, Sarah Spiekermann 2001, Jens Grossklags 2005

[167] Cfr, http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#431

28mila cittadini Europei ai quali è stato chiesto di esprimere una valutazione circa la protezione dei propri dati personali[168]. Si riportano, a seguire, i grafici aggregati e in didascalia la deduzione emergente.

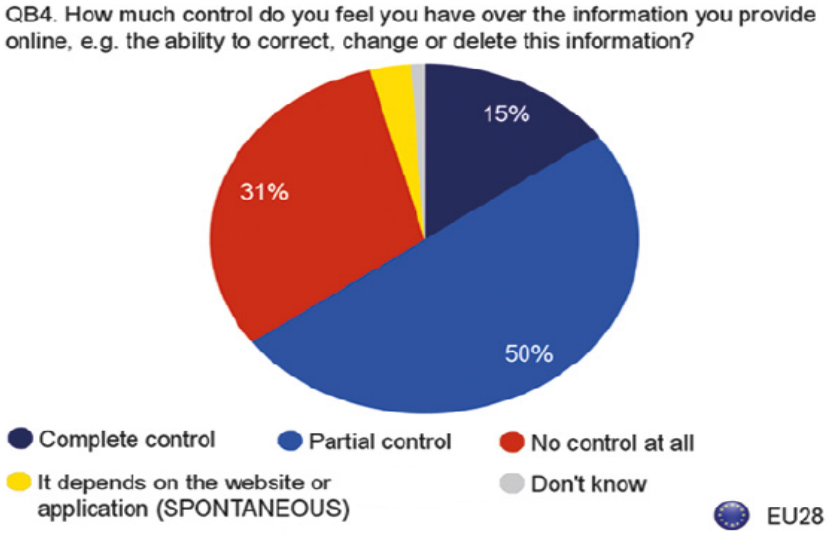


Figura 2.12 - Percezione di controllo sui dati personali
Due terzi degli intervistati (67%) ritiene di non avere il controllo completo delle informazioni rilasciate on-line.

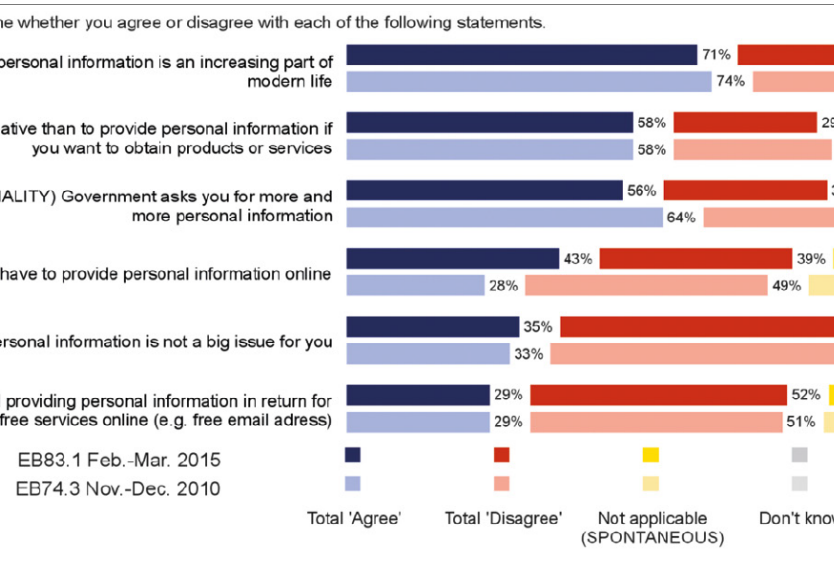


Figura 2.13 – Divulgazione dei dati personali
La maggioranza degli intervistati (71%) sostiene che fornire informazioni personali on line ha un'importanza crescente anche in ragione dell'assenza di alternative rispetto all'accesso ai servizi richiesti.

[168] In argomento la versione integrale del report è disponibile alla seguente risorsa: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf

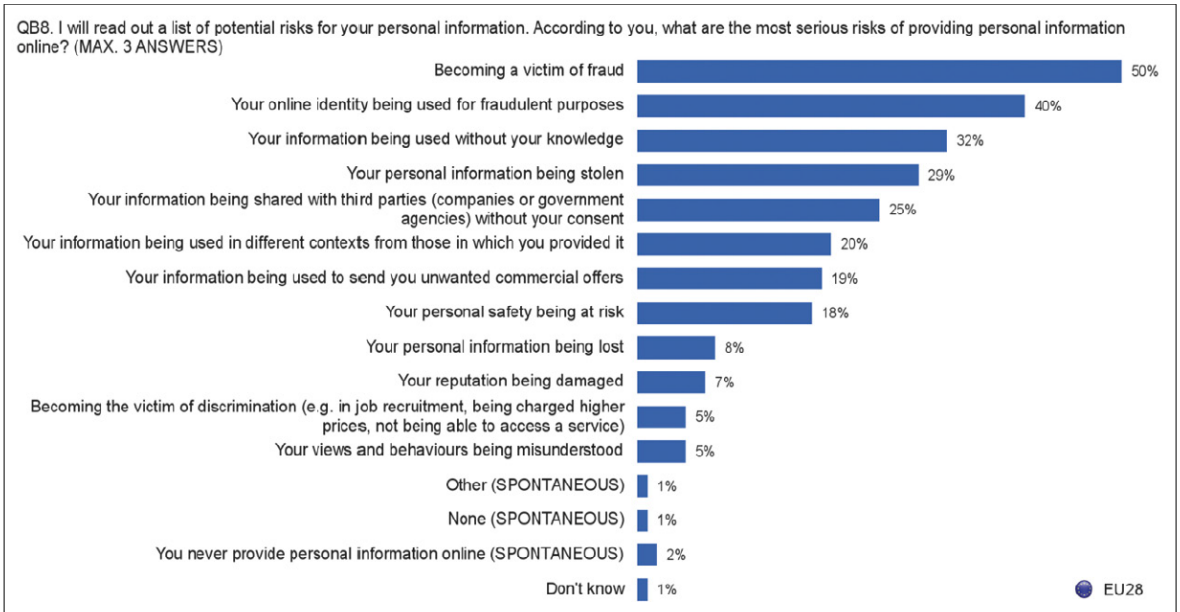


Figura 2.14 – Rischi e responsabilità relative alle informazioni personali fornite online

Subire una frode on-line, l'utilizzo illecito e non informato delle proprie informazioni risultano il reato più grave rispettivamente per il 50%, 40% e 32% degli intervistati.

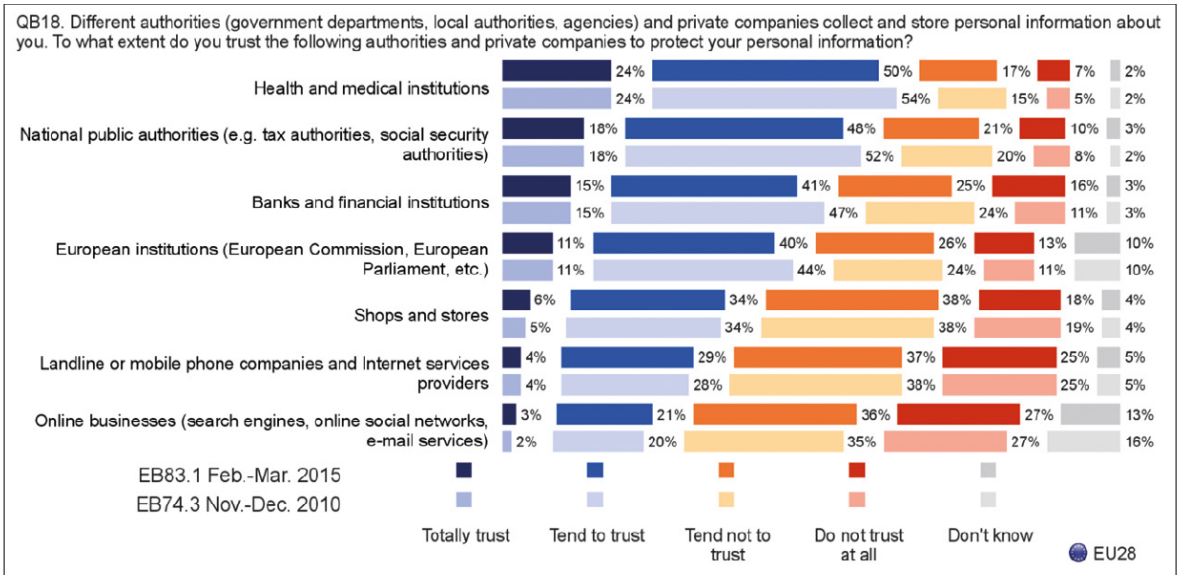


Figura 2.15 – Percezione del rischio connesso alla gestione di dati personali da terze parti

Il 69% degli intervistati ritiene che il consenso debba essere richiesto in forma esplicita prima che i dati siano raccolti e trattati. Inoltre 7 intervistati su 10 mostrano preoccupazioni in merito al fatto che i dati personali siano utilizzati per scopi diversi da quelli associati alla raccolta.

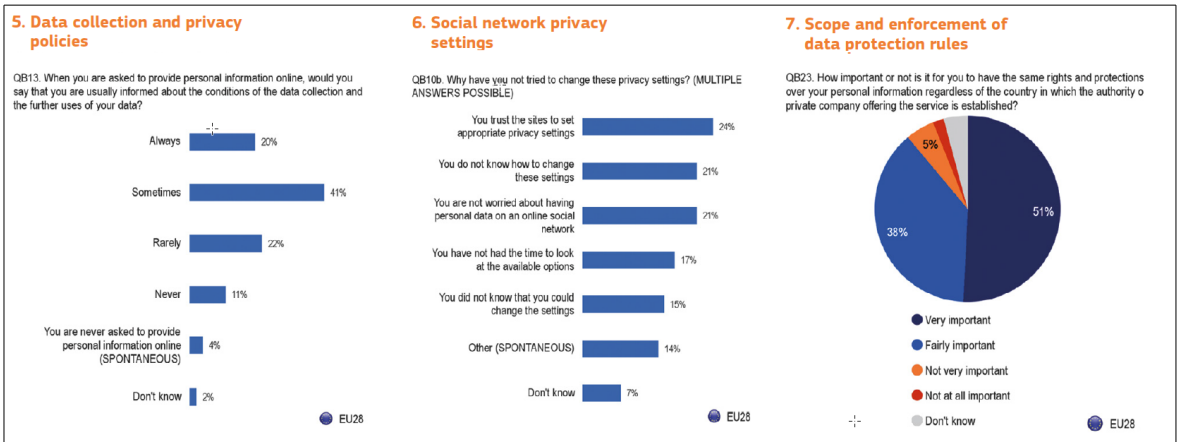


Figura 2.16 – Gestione delle politiche di privacy

1 su 5 degli intervistati dichiara di conoscere come i dati personali sono collezionati e utilizzati avendone letto le condizioni di utilizzo. Inoltre il 50% degli intervistati ha tentato di personalizzare le impostazioni di privacy e tra questi i 3/4 ha ritenuto questo passaggio un'operazione semplice; il complementare 50% ritiene il passaggio non necessario o non semplice. Infine la maggior parte degli intervistati ritiene che a livello normativo nell'Unione la protezione dei dati personali debba essere trattata in modo centralizzato e uniforme.

In linea agli esiti delle rilevazioni dell'Eurobarometro, secondo uno studio della *McCann Truth Central*[169] - svoltosi nel 2011, specificatamente orientato ai Social Media e con un coinvolgimento di 6mila utenti provenienti da 6 paesi diversi, il 70% delle persone intervistate evidenzia preoccupazioni per la propria *privacy* online. In contrasto però solo il 50% delle persone si astiene dall'aggiungere amici o contatti che non conosce, e una percentuale ancora minore ha personalizzato le regole di privacy.

La conclusione generale che può essere ricavata è che tendenzialmente gli utenti, pur sempre più preoccupati per la propria *privacy,* si aspettano che sia il sistema, il fornitore del servizio o il titolare a proteggere i propri dati. Tale preoccupazione – di per se legata più al verificarsi *ex- post* di un evento dannoso (e alle perdite personali che ne derivano) che ad una preventiva e consapevole conoscenza di minacce e rischi, può essere abbattuta e compensata in cambio di piccoli sconti e compensazioni vantaggiose monetarie e non[170].

Diffidenza e preoccupazione non sono seguite da azioni volte a schermare il *dislosure* delle informazioni valutando e filtrando quelle necessarie da quelle ridondanti; l'invocazione di *privacy* viene smentita dall'effettivo comportamento dell'utente, permanendo una forte

[169] McCann Truth Central. *The truth about privacy. executive summary,* (2011) http://truthcentral.mccann.com/about/

[170] Sull'argomento si indicano gli esperimenti descritti in: SPIEKERMANN S., GROSSKLAGS J., BERENDT B., *E-privacy in 2nd Generation Ecommerce: Privacy Preferences Versus Actual Behavior*, Proceedings of the ACM Conference on Electronic Commerce (EC '01), p. 38-47, 2001.

disponibilità a rivelare e diffondere *on-line* e *sui social media* dati personali anche molto privati o addirittura sensibili; si configura in definitiva una disconnessione tra ciò che l'utente pensa – preoccupazione, sfiducia, dubbi, diffidenza e ciò che l'utente fa e sceglie: una dicotomia tra le sue *attitudini* e l'effettivo suo *comportamento.*

Al configurarsi di questo *gap* possono concorrere diverse ragioni: i costi e le difficoltà di utilizzo delle tecniche di protezione[171]; la difficoltà ad introdurre cambiamenti nel proprio comportamento in termini di regole e preferenze di utilizzo e divulgazione dei propri dati; l'ignoranza verso i rischi occorrenti nella gestione dei dati personali; la rinuncia dettata dalla convinzione dell'impossibilità di proteggersi contro ogni tipo di invasione; la tendenza verso la gratificazione immediata; il disinteresse e il distacco verso le soluzioni di protezione proposte: solo pochi degli utenti che accettano e sottoscrivono i termini di utilizzo dei propri dati effettivamente ne conoscono il contenuto e le implicazioni[172], permanendo quindi una complessiva scarsa visibilità sulle regole e sulle decisioni attuate; la difficoltà stessa delle aziende di fornire soluzioni tecnologiche di protezione semplici ed efficaci che riscontrino con immediatezza tanto le aspettative degli utenti tanto gli effetti e le implicazioni pratiche di una specifica impostazione.

La divergenza tra attitudine e comportamento dipende, inoltre, molto dal contesto (*context-dependent);* su di essa incide in modo significativo come:

- ✔ la questione *privacy* viene pre-configurata e proposta all'utente - ovvero lo *status quo,* il dominio di *default settings* proposto all'utente;
- ✔ nonché la misura e l'impatto della trasparenza (quindi l'informativa e *privacy notice)* esposta all'utente; e
- ✔ la tipologia degli strumenti di controllo di cui questi dispone (quindi consenso e *privacy settings).*

Su questo argomento si distinguono le sperimentazioni in tema di economia della *privacy* ed economia comportamentale della *privacy* effettuate presso la Carnegie Mellon University

[171] In argomento: BRUNK B.D. In *Understanding the Privacy space*, First Monday, vol. 7, n. 10. http://www.firstmonday.org/issues/issue7_1O/brunk/ index. html, 2012 – rileva e documenta come poche delle tecnologie *Pets* a diretto controllo dell'utente (ad esempio basate su infrastrutture PKI certificate) abbiano trovato diffusione e successo nel mercato o abbiamo riscontrato livelli di adozione significativi

[172] STUTZMAN F., CAPRA R., THOMPSON L., *Factors mediating disclosure in social network sites*. Computers in Human Behavior, 27(1):590 – 598, 2011. Third International Cognitive Load Theory Conference.
http://www.sciencedirect.com/science/article/pii/S0747563210003158, doi:10.1016/j.chb.2010.10.017
In questo contributo gli autori documentano un problema di comunicazione e trasparenza nelle Privay Notice dei più diffusi Social Media ed in particolare la difficoltà anche per gli utenti più consapevoli di cogliere con immediatezza le implicazioni e gli effetti delle impostazoni di *privacy.*

(Pittsburgh, Pennsylvania, USA) dal gruppo di ricerca del prof. Alessandro Acquisti[173]. Di seguito viene illustrata l'incidenza assunta nelle decisioni di *privacy* da fattori quali: *i)* il *default settings* ovvero il contesto iniziale in cui inizialmente l'utente gestisce i propri dati personali; e *ii)* gli strumenti di protezione: trasparenza e controllo, di cui dispone.

Nel corso di una sperimentazione finalizzata a comprendere se e su quanto gli utenti fossero disponibili a spendere per la protezione dei propri dati - suddivisi in due gruppi i partecipanti ad una rilevazione (apparentemente non attinente al tema *privacy),* ad ognuno di essi – viene regalata una carta prepagata: con 10 dollari di credito e mantenimento dell'anonimato negli acquisti, per un gruppo; con 12 dollari e identificazione, per l'altro gruppo. Trascorso qualche minuto, dopo la consegna della carta, ai membri di entrambi i gruppi viene proposto lo scambio di carte: l'insieme delle scelte è identico (essere disponibili a sostenere un costo di 2 dollari) ciò che cambia sono le condizioni iniziali (lo *status quo,* il *default settings).* Risultati: il 51% degli utenti del primo gruppo rifiuta lo scambio, analogamente il 91% degli utenti del secondo gruppo. Gli utenti del primo gruppo partono da una situazione di disponibilità di *privacy,* il convincimento a rinunciarvi e a rilasciare i propri dati per compensazione monetaria è *esterno,* la metà degli utenti lo rifiuta o lo ritiene inadeguato. Gli utenti del secondo gruppo, per impostazione predefinita, non dispongono della *privacy,* la spinta motivazionale ad acquisirla per rinuncia/costo monetario è *interna* e pochi sono disposti a pagare 2 dollari. Questo esperimento evidenzia come la disponibilità di *default* della privacy sollecita a valutarne diversamente il valore - in misura maggiore o minore.

Default Settings: *circolo virtuoso/vizioso della protezione dei dati personali*

quando le condizioni iniziali già configurano una posizione di protezione tendenzialmente gli utenti sono più propensi ad attribuire più valore ai propri dati personali; viceversa nella situazione situazione opposta, i dati personali sono valorizzati in maniera minore con conseguente propensione a rilasciarli più facilmente.

La **trasparenza e il controllo** sono strumenti di protezione della circolazione dei dati personali tanto in contesti regolatori autoregolamentati e settoriali (come quello americano) tanto generalisti e centralizzati (come quello europeo); rispetto alla *privacy* e alla protezione dei dati personali e in relazione al comportamento dell'utente in fase di *disclosure,* trasparenza e controllo si rivelano condizioni necessarie (quindi più controllo, più trasparenza => più privacy) ma non sufficienti[174] (quindi più controllo, più trasparenza => meno privacy).

L'inversa proporzionalità tra controllo e *privacy* si verifica quando, per esempio, comparando il rilascio del medesimo *data set*[175]*,* sotto vincolo di autorizzazione implicita (quindi con preconfezionato e limitato controllo) o alternativamente esplicita (quindi con

[173] In argomento di rimanda alla consultazione degli atti Lectio Magistralis Prof. Alessandro Acquisti – Privacy nell'era del DataGeddon 19 Giugno 2014, CNR Pisa, disponibili alla risorsa: https://www.federprivacy.it/component/videoflow/?task=play&id=224

[174] ACQUISTI ALESSANDRO, *The Economics of Personal Data and the Economics of Privacy,* Year: 2010, OECD Privacy Guidelines, p.6 Atti Lectio Magistralis Prof. Alessandro Acquisti – Privacy nell'era del DataGeddon 19 Giugno 2014, CNR Pisa, disponibili alla risorsa: https://www.federprivacy.it/component/videoflow/?task=play&id=224

[175] Ad esempio sotto forma di risposte a questionari valorizzate con dati personali o sensibili.

maggiore controllo), si rileva che l'utente – in quest'ultimo caso, tende a rilasciare un maggior numero di dati personali, anche sensibili. Un maggior controllo può quindi esercitare una sorta di processo di *empowerment* sull'utente, innescando un meccanismo di *over - confidence* in base al quale l'utente rilascia più dati, configurando – potenzialmente, più rischi con conseguente decremento della *privacy.*

Analogamente per la trasparenza: invertire la consolidata tendenza di esporre informative *(privacy notice)* lunghe, arcane nella forma e ambigue nella sostanza ricorrendo, invece, ad informative complete, chiare ed efficaci nelle implicazioni, può favorire nell'utente una reazione coerente e razionale, per esempio inibendo il rilascio di dati personali altrimenti divulgati; tendenzialmente, tuttavia, questo accade quando l'esposizione e la comunicazione delle regole di utilizzo (per quanto chiare ed efficaci) si mantengono compresenti e affiancate alla fase di *disclosure* delle informazioni, perdendo quindi la loro portata e la loro ***salienza*** se si introduce un differimento temporale tra la comunicazione dell'informativa e il rilascio delle informazioni[176]. Quindi al miglioramento quantitativo (più informativa) e qualitativo (più chiarezza ed efficacia) non sempre corrisponde il mantenimento di un altrettanto migliorato ed efficace *disclosure* delle informazioni personali (per minimizzazione dei dati e differenziazione della tipologia) se la l'aumento di trasparenza non è seguita dal mantenimento, nel tempo, dalla *salienza* e dalla *prominenza* delle condizioni di utilizzo descritte ed esposte all'utente.

Per quanto illustrato e ricollegando alle domande iniziali, rispondere se per i soggetti interessati la *privacy* è una questione importante o meno richiede una valutazione molto complessa e tutt'ora aperta, che sarebbe oltre che errata estremamente pericoloso ridurla ad un binario si/no.

Le persone provano un nativo bisogno di comunicare, di partecipare, di esporsi e questo passa inevitabilmente attraverso il *disclosure* delle proprie informazioni (immagini, stato), del proprio pensiero, dei propri luoghi. Al contempo le persone avvertono (in misura sempre crescente) un bisogno di *privacy* e di protezione per la propria sfera individuale.

I due bisogni non sono in contraddizione, pensarle come tali e ritenerli due mondi separati e inconciliabili (o l'uno o l'altro, oppure il *disclosure* pregiudica la *privacy)* rappresenta una fuorviante semplificazione del problema.

Ciò che cambia è il contesto in cui si sviluppano questi due elementi e in cui l'utente si

[176] Atti Lectio Magistralis Prof. Alessandro Acquisti – Privacy nell'era del DataGeddon 19 Giugno 2014, CNR Pisa, disponibili alla risorsa: https://www.federprivacy.it/component/videoflow/?task=play&id=224

trova a prendere decisioni verso la divulgazione o verso la protezione dei propri dati personali:

- ✔ il primo: semplice, vantaggioso, diretto, non costoso, gratificante, che incrocia e costruisce direttamente la *user-experience*[177], grazie soprattutto alla pervasività e all'immediatezza dei s*ocial media* e delle *mobile apps;* questo contesto esplicita, con completezza e immediatezza, all'utente tutte le informazioni necessarie, per lo più esposte come vantaggi e benefici derivanti dal rilascio dei propri dati personale di cui l'utente può calcolarne e valutare la dimensione con un ritorno di utilità contestuale e tempestivo.
- ✔ il secondo: articolato, mediato da tecnologie di protezione non native ma aggiunte, che richiede valutazione e comparazione - quindi costoso, differito dalla *user-experience;* questo contesto, inoltre, si distingue per *informazione incompleta*, *razionalità limitata* e *deviazione sistemantica*[178] incidendo negativamente sulle decisioni di *privacy,* che quindi vengono spesso omesse o delegate a chi fornisce il servizio; in questo scenario l'utente dopo aver fornito ad altre parti le proprie informazioni ne perde letteralmente e indefinitamente il controllo.

In conclusione l'utente (la persona, il soggetto interessato) è un attore centrale tanto nella divulgazione quanto nella protezione delle proprie informazioni, che però prende le rispettive decisioni in contesti informazionali molto diversi. Quando l'utente affronta le decisioni decisioni di *privacy* raramente dispone di tutte le informazioni necessarie, se comunque le avesse riscontrerebbe difficoltà ad analizzarle in maniera completa e accurata, e anche se così non fosse divergerebbe dalla scelta ottimale (al limite andando contro i propri interessi).[179]

Le contromisure di *Privacy Enhancing Technologies* di tipo proattivo – ovvero rispondente ai requisiti di *Privacy by Design* ed in particolare a quello *user-centric* implementato tramite

---

177 L'ISO 9241-210:2010, *Ergonomics of human system interaction - Part 210: Human-centered design for interactive systems.* definisce l'esperienza d'uso come "le percezioni e le reazioni di un utente che derivano dall'uso o dall'aspettativa d'uso di un prodotto, sistema o servizio". L'esperienza d'uso è soggettiva e si concentra sull'atto dell'utilizzo.

178 Queste argomentazioni - per il rilievo che assumono in ambiti informazionali in cui tanto le transazioni di dati personali tanto le violazioni sono onnipresenti e invisibili, saranno disaminate in dettaglio nel capitolo 4 - *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.* Esse attengono: *i)* la omessa esplicita descrizione dei rischi e delle violazioni connesse ad una determinata transazione, nonché delle possibili contromisure per prevenire, contenere o rispondere alle implicazioni negative (informazione incompleta); e *ii)* l'incapacità per l'utente di confrontare e misurare – tanto in fase di divulgazione delle proprie informazioni tanto nel tempo, la dimensione e lo spessore dei benefici associati alle varie e possibili strategie adottabili per la protezione della *privacy; iii)* lo scostamento, pur in condizioni informative complete, dalla decisione di privacy

179 Questa circostanza si verifica soprattutto quando l'utente, nel processo decisionale *disclosure* vs *privacy,* reagisce secondo la logica dello sconto iperbolico (favorito da sottostima delle criticità, gratificazione immediata e non autocontrollo): in presenza di un beneficio immediato (sconto sul prezzo di un bene, compensazione monetaria o crediti di varia natura come contropartite al rilascio di dati personali) l'utente decide *nell'immediato* di rilasciare i propri dati, consapevole di accettare *in prospettiva* un costo molto maggiore connesso ad un rischio per quanto futuro e potenziale (ad esempio furto di credenziali di credito rilevate in quella transazione).

framework di politiche, possono supportare e rispondere a queste questioni. Alla disamina delle caratteristiche di questa tipologia di contromisure è dedicato il prossimo capitolo 3 - *Privacy e Protezione dei Dati personali: le contromisure.*

CAPITOLO 3

PRIVACY E PROTEZIONE DEI DATI PERSONALI: LE CONTROMISURE.

SOMMARIO: 1. Tecnologie per la protezione dei dati e delle informazioni personali. – **1.1** *Public Key Infrastructure:* brevi cenni. – **2.** *Privacy-Enhancing Technologies.* – **2.1.** L'anonimato e la protezione dei dati personali. – **2.1.1.** L'analisi tecnico-giuridica del trattamento di anonimizzazione. – **2.1.2.** Le tecniche di anonimizzazione. – **2.1.3.** La pseudonimizzazione. – **2.1.4.** Il diritto all'anonimato: profilo e identificabilità della persona. – **3.** I sistemi di *Privacy Policies - Preferences.* – **3.1.** Le *Privacy Policies* di tipo *"provider centered".* Esempi. – **3.2.** Le *Privacy Policies* di tipo "*User-centric"* e *"Data-centric". Sticky Privacy Policies. Privacy Proxies.* – **3.3.** I Framework e i linguaggi. – **4.** Questioni aperte. – **5.** La protezione dei dati personali come requisito intrinseco di processi e servizi. – **5.1.** Il framework *Privacy by Design* e P*rivacy by Default.*

1. TECNOLOGIE PER LA PROTEZIONE DEI DATI E DELLE INFORMAZIONI PERSONALI.

Le misure per la protezione delle informazioni digitali (e dei dati personali) possono essere raggruppate in tre categorie principali: *i)* misure di sicurezza, *ii)* misure di *privacy, iii)* misure basate su politiche. Le misure di sicurezza sono specificatamente finalizzate alla tutela dei requisiti di confidenzialità o riservatezza, integrità, autenticità e disponibilità.

Le misure di *privacy* sono volte alla protezione delle informazioni personali ed in particolare tutelano l'associazione identificativa [dato, persona], sono etichettate con il termine *Privacy-Enhancing Technologies (PETs).*

Le misure basate su politiche utilizzano regole di controllo degli accessi e delle autorizzazioni all'utilizzo dei dati.

1.1 PUBLIC KEY INFRASTRUCTURE: BREVI CENNI.

Le misure di sicurezza a seconda dell'ambito di intervento si differenziano in misure di sicurezza di livello fisico (sistema e rete, comprendenti: antivirus, antispyware, sistemi di backup e di intrusion detection system, firewall, protocolli sicuri e sistemi di perimetrazione di rete, Virtual Private Network) o di livello logico (applicazioni, comprendenti: sistemi di cifratura, firma digitale, autenticazione, di steganografia e watermarking).

Per molti utilizzi entrambe le categorie condividono l'utilizzo della crittografia, essa

rappresenta il processo di creare e decifrare comunicazioni segrete. Dati personali criptati sono trasformati in codici non interpretabili senza una chiave segreta, quindi protetti a seconda che siano trasmessi in rete, conservati su computer o dispositivi, archiviati in banche dati.

Gli algoritmi di crittografia si dividono in due principali categorie: algoritmi reversibili e irreversibili[180] a seconda sia possibile ricodificare il dato originario a partire da quello cifrato.

Gli algoritmi di cifratura sono funzioni note, la segretezza del processo è interamente contenuta nella chiave di codifica, la robustezza un indicatore *relativo* dipendente dalla capacità computazionale, dalle risorse e dai tempi necessari per la decifratura: rompere un algoritmo di cifratura non è un'operazione impossibile in senso assoluto ma semplicemente molto costosa.

Gli algoritmi di cifratura reversibili si distinguono in simmetrici e asimmetrici (a chiave pubblica), a seconda che le operazioni di cifratura e decifratura siano eseguite utilizzando, rispettivamente, una singola chiave oppure una doppia chiave (pubblica per cifrare e privata per decifrare, comunque biunivocamente associate).

Le infrastrutture a chiave pubblica *(PKI, Public Key Infrastructure)* sono sistemi applicativo/gestionali volti a garantire - mediante certificazione di una terza parte fidata (cd. Certification Authority), l'appartenenza della coppia di chiavi (pubblica e privata) al legittimo utilizzatore; consentono di divulgare la chiave pubblica mediante una credenziale digitale (certificato digitale) e mantenendo segreta quella privata. Le catene di certificazione possono essere gerarchiche[181] oppure a rete in cui i singoli utenti sono collegati da una relazione di fiducia bilaterale[182]. Le *PKI* e i certificati digitali sono alla base del funzionamento di tutte le applicazioni crittografiche - dai protocolli sicuri (*SSL, Secure Socket Layer* o *IPsec, IP security*) alla firma digitale, la cui implementazione e il cui funzionamento sono configurati in standard internazionali consolidati[183].

La cifratura dei dati personali tuttavia di per se e da sola non risolve ogni problema di *privacy;* l'utilizzo di dati cifrati non può essere unilaterale: un utente non può inviare dati personali protetti tramite crittografia se il destinatario non li accetta in tale forma ed è in grado di decifrarli; una volta decifrati i dati non sono più protetti, quindi nuovamente incontrollati.

---

[180] Gli algoritmi irreversibili sono funzioni (note) che producono un'impronta del dato di lunghezza costante (indipendentemente dall'informazione originaria), non soggetta a collisioni (quindi solo dati uguali producono medesime impronte) e dalla quale è *computazionalmente impossibile* ricavare il dato iniziale in tempi *ragonevoli* e risorse *proporzionate.* Le funzioni di hash sono gli algoritmi irreversibili più diffusi e utilizzati per verificare l'integrità dell'informazione disponendo dell'originale cfr .https://it.wikipedia.org/wiki/Hash

[181] Cfr https://it.wikipedia.org/wiki/X.509,

[182] Cfr https://it.wikipedia.org/wiki/Pretty_Good_Privacy

[183] Cfr https://italy.emc.com/emc-plus/rsa-labs/standards-initiatives/public-key-cryptography-standards.htm

2. PRIVACY-ENHANCING TECHNOLOGIES.

Le tecniche di cifratura sono usate in un numero crescente di protocolli ed applicazioni che non mascherano semplicemente i dati, ma aiutano a salvaguardare la *privacy* di una persona in diverse tipologie di situazioni, intervenendo sull'associazione di identificabilità: è possibile concludere transazioni confidenziali con parti terze sconosciute; completare pagamenti elettronici senza rivelare dati finanziari; inviare messaggi elettronici non riconducibili al mittente; navigare su Internet senza rivelare i siti visitati o il dispositivo utilizzato; votare elettronicamente conciliando correttezza del voto e segretezza della preferenza; condividere contenuti ed interessi con altri utenti senza rivelare la propria identità, utilizzare sistemi di credenziali anonime.

Alcuni di questi protocolli separano i dati personali identificabili da quelli non riconducibili all'individuo, altri puntano a proteggere la *privacy* rompendo l'associazione identificativa tra il dato, il suo significato (quindi l'azione o il fenomeno veicolato) e l'utente, altri puntano a minimizzare a priori l'utilizzo di dati personali.

Nel loro complesso le misure utilizzate specificatamente per proteggere le informazioni personali sono note come *Privacy-Enhancing Technologies (PETs):* tecnologie per il miglioramento della *privacy.*

Rispetto alle misure di sicurezza logica intese in senso stretto e con riferimento alla crittografia reversibile ed irreversibile, le *PETs* intervenendo sui dati personali, separandoli o disconnettendoli dal resto dei dati di trattamento, consentono di proteggerne tanto il processamento e la gestione, tanto l'identificabilità del soggetto interessato senza interrompere la divulgazione di informazioni necessarie al completamento di una transazione.

La definizione più consolidata individua nelle *PETs* un sistema coerente di misure tutela la *privacy* eliminando o riducendo i dati personali, ovvero evitandone un qualunque trattamento non necessario e/o indesiderato ma preservando al contempo la funzionalità del sistema di informazione[184].

Le *PETs* sono state introdotte dalla Commissione europea nell'ambito delle iniziative volte allo sviluppo delle tecnologie di rafforzamento della tutela della vita privata, con lo scopo di prevenire i rischi derivanti da un uso fraudolento dei dati personali, contribuire all'ideazione di sistemi e servizi di informazione e comunicazione che permettono di ridurre al minimo la

[184] cfr GÜRSES SEDA, *PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm,* Identity in the Information Society, December 2010, Volume 3, Issue 3, p. 539-563 (2010).

raccolta e l'uso di dati personali, favorire il rispetto delle norme sulla protezione dei dati; contrastare i furti di identità, le frodi e la profilazione discriminatoria. Le principali misure di *PETs* comprendono l'anonimizzazione e la pseudonimizzazione[185].

2.1. L'ANONIMATO E LA PROTEZIONE DEI DATI PERSONALI.

L'*anonimizzazione* è quel processo elaborativo che – applicato ad un determinato insieme di dati personali e nel contesto di una determinata attività informazionale ne interrompe l'associazione (diretta o indiretta) con il soggetto interessato, puntando quindi ad una de-identificazione irreversibile; è un processo che non implica necessariamente l'oscuramento o la codifica di informazioni digitali - rappresentanti comportamenti, azioni, fatti o attività dell'interessato, originariamente in chiaro e che rimangono, pertanto, *aperte* e riutilizzabili per le prefissate finalità di processamento - ma ne blocca la riconducibilità identificativa con la persona che li ha compiuti o alla quale si riferiscono[186].

In tal senso l'*anonimizzazione* non deve essere assimilata a misure volte alla protezione della divulgazione di informazioni o di dati personali per finalità segretezza o confidenzialità dei contenuti (quali, ad esempio la cifratura). Parimenti deve essere distinta dalla *pseudonimizzazione* – processo che blocca la correlabilità dei dati personali all'identità di una persona ma che non produce un insieme di informazioni anonime, con conseguente possibile re-identificazione del soggetto interessato.

L'*anonimizzazione,* come sarà meglio illustrato nel seguito, è un processo intrinsecamente relativo rispetto alla irreversibilità della de-indentificazione - fattore dinamicamente dipendente dal grado di sviluppo e di disponibilità (crescente) delle tecnologie, dalle risorse (tempi e costi) necessari per il loro utilizzo (decrescenti) il tutto contestualizzato all'atto del trattamento. Contesto che oggi è quello del *DataGeddon* e *data intensive* in cui il massivo utilizzo e l'accresciuta disponibilità di informazioni ne aumenta il potenziale di collegabilità e inferenza, e in cui la ricostruzione del profilo di una persona può avvenire per via indiretta senza senza l'ausilio immediato o diretto di dati identificativi.

Sull'argomento è indicativo rilevare l'approccio "realistico" del GDPR (rispetto al CODICE) nell'articolare la *pseudonimizzazione*[187] in luogo della *anomimizzazione*, in un certo

[185] cfr GÜRSES SEDA, *PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm,* Identity in the Information Society, December 2010, Volume 3, Issue 3, p. 544-546

[186] In argomento si indicano: a) i pareri Working Party ex art. 29 n. 216 - Opinion 05/2014 *on Anonymisation Techniques* 10 Aprile 2014 pag. 5-6; 9-11 (IT). b) e n. 136 - Opinion 4/2007 *on the concept of personal data*, 20 Giugno 2007 pag. 21.

[187] Il GDPR all'art.4 Definizioni comma 5 così definisce la *pseudonimizzazione:: il trattamento dei dati personali in modo tale che i dati*

senso risolvendo a priori una intrinseca criticità e al contempo mantenendo un certo grado di neutralità delle norme rispetto ai più rapidi cambiamenti tecnologici.

L'*anonimizzazione* può essere considerato a tutti gli effetti come un trattamento successivo dei dati personali - come tale oggetto di verifica della compatibilità dei presupposti giuridici di liceità – art. 6 del GDPR *Principi applicabili al trattamento di dati personali*; del contesto e delle finalità, dei principi di qualità dei dati – art. 5 del GDPR *Liceità del trattamento* e art. 11 del CODICE *Modalità di trattamento e requisiti dei dati*.

In argomento il CODICE e il GDPR sostengono con intensità diverse il diritto del soggetto interessato alla de-identificazione - quindi alla tutela del proprio anonimato o pseudonimato: per il CODICE è un requisito strutturale *forte* di gestione delle informazioni digitali, tale da poter escludere il trattamento stesso di dati personali in una ideale applicazione del principio di necessità – cfr art. 3 *Principio di necessità nel trattamento dei dati* comma 1), ogni qual volta sia possibile perseguire le prefissate finalità attraverso l'utilizzo di dati anonimi[188].

Per il GDPR le informazioni anonime sono una tipologia di dati non soggette ai principi di protezione, mentre la *pseudonimizzazione* è vera e propria misura di sicurezza di tipo *privacy by design* strumentale all'attuazione del principio di *minimizzazione*[189], una garanzia (tra le altre e in contingenza di differenti finalità) di liceità del trattamento – cfr art. 6 *Liceità del trattamento*, comma 4, lettera 6) *...dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*.

A rigor di definizione deducibile incrociando sull'argomento: *i)* il GDPR – considerando

personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

[188] CODICE, Art. 3 comma 1 Principio di necessità nel trattamento dei dati *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.*

[189] GDPR art. 25 P*rotezione dei dati fin dalla progettazione e protezione per impostazione predefinita* comma 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.*

26)[190] per il ricorso alle tecniche di *pseudonimizzazione*[191] in luogo di quelle di *anonimizzazione,* ma che nel *considerando* le riconosce e ne contestualizza la intrinseca relatività; e *ii)* il CODICE – che non definisce la *pseudonimizzazione* e si distingue per la circostanza opposta, ovvero nel premettere la esplicita definizione di dato anonimo[192] - l'*anonimizzazione* è, quindi, un trattamento successivo, volto a impedire irreversibilmente l'individuazione della persona, basato sul principio di sottrazione e minimizzazione dei dati identificativi; può ritenersi una estrema forma di minimizzazione dei dati al punto da non consentirne più l'identificazione diretta o indiretta[193].

È un processo intrinsecamente relativo che tende probabilisticamente a falsare il collegamento associativo e tra i dati personali e la persona; al limite, una (ideale) corretta implementazione dell'*anonimizzazione* dovrebbe avere una probabilità di attribuzione pari a quella del tutto casuale che comunque si avrebbe in assenza del dato anonimizzato.

I dati personali oggetto di un trattamento di *anonimizzazione* – che tipicamente sono dati importanti per la persona, es. dati privati (economici) o sanitari, perdono la prerogativa di riferirsi ad una persona identificata o identificabile, ciò comunque rispetto a variabili contestuali quali il tempo, le risorse e lo stato di avanzamento dei mezzi tecnologici che – a tal fine, possono essere *ragionevolmente* essere impiegati: una sorta di (ipotetica quanto relativa) permanente cancellazione dei dati personali identificativi, ovvero (così come premesso nelle definizioni del CODICE) di quel particolare sottoinsieme di dati personali strumentali alla identificazione *diretta* dell'interessato[194] - e quindi tale da rendere *impossibile* qualsiasi altro trattamento.

Alle informazioni rese anonime non si applicano le disposizione sulla protezione dei dati

---

[190] GDPR, considerando 26): *dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.* ***Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.***

[191] GDPR art. 4 Definizioni, comma 4: *«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.*

[192] CODICE, Art. 4 - Definizioni, comma 1, lettera n): "*dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

[193] D'ACQUISTO G., NALDI M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017), pag 34-35.

[194] CODICE, Art. 4 - Definizioni, comma 1, lettera c): *"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato*

personali venendo meno il necessario presupposto identificabilità - considerando 26) del GDPR[195]. Ne consegue che sui dati *veramente* anonimizzati vengono meno le questioni e i vincoli relative alle finalità perseguite, al consenso e all'informativa.

Questa osservazione non è retorica e assume importanza nell'ambito della configurazione normativa di quei trattamenti di dati personali posti in essere in contesti di raccolta voluminosa, con informazioni provenienti da fonti eterogenee (*Big Data*, in particolare; e *IoT*) ed indirizzate a profilazioni individuali e sociali, in cui il differenziarsi delle finalità è una imprescindibile caratteristica intrinseca.

L'eccezione ai vincoli del GDPR di cui al considerando 26) consentirebbe – ad esempio, a rendere trattamenti di tipo *Big Data* pienamente conformi alla normativa solo se effettuati su dati *anonimizzati*, anche se in contingenza di una relativa quanto incerta attuazione pratica se si considera la finalità gestionale predittiva e di profilazione propria tali processi informazionali. Su questo aspetto si rimanda al successivo capitolo 4, *Verso la Privacy 2.0: nuovi scenari di rischio e nuove semantiche.*

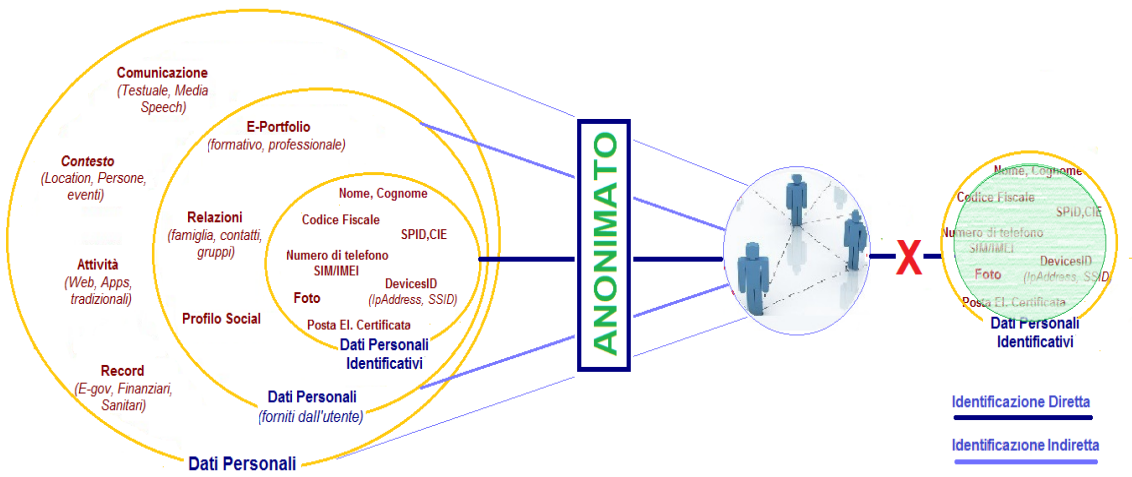


Figura 3.1 - Trattamento di *anonimizzazione*

Il trattamento di *anonimizzazione* interviene sulla relazione associativa che intercorre tra la persona (identificata o identificabile) e l'insieme dei dati personali, falsandone e rendendone particolarmente incerta (al limite impossibile) l'attribuzione, al punto di simulare gli stessi effetti di una ideale permanente cancellazione (logica) dei dati identificativi tale da avere una probabilità di attribuzione pari a quella del tutto casuale che comunque si avrebbe in assenza del dato *anonimizzato*.

[195] Anche sotto questo profilo il GDPR assume un approccio più relativo e meno rigoroso rispetto all'utilizzabilità dei processi di *anonimizzazione* (che non si esclude si possa leggere come un riconoscimento più forte verso le tecniche di data mining e quindi di profilazione): nelle premesse al considerando 26) esclude dal trattamento i dati anonimi, nell'articolato si riferisce a dati pseudoanonimizzati, quindi dati identificabili il soggeto e - come tali, dati personali ricadenti nell'ambito materiale del GDPR.

Un efficace processo di *anonimizzazione* impedisce a tutte le parti interessate di identificare una persona in un insieme di dati rappresentanti determinati eventi, attività, comportamenti nel presupposto che con il termine identificazione non si intenda solo la concreta possibilità di ricavare dati identificativi come il nome o il telefono, ma anche la potenziale (indiretta) identificabilità mediante correlazione e deduzione.

In generale l'eliminazione di dei dati identificativi non è, quindi, sufficiente a garantire l'irreversibilità della de-identificazione[196], occorre quindi adottare misure ulteriori e supplementari che tengano conto non solo della persona ma del contesto di trattamento: attività e finalità.

> ***Esempio:*** Supponiamo che un'azienda titolare del trattamento raccolga dati sugli accessi delle persone a Internet o ad un servizio specifico (ad esempio - in WhatsApp Messenger, l'accesso al relativo sistema di messaggistica mediante l'App scaricata sullo smartphone del soggetto interessato[197]). Per la configurazione del trattamento di anonimato concorrono i seguenti presupposti: a) la tipologia dell'evento o di attività, quindi, ad esempio: *accesso individuale giornaliero;* b) i dati (personali) di accesso, quindi ad esempio, almeno: *data e ora*; c) il soggetto interessato in quanto tale, quindi: *Mario Rossi*; d) i dati (personali) identificativi, quindi ad esempio: *nome_utente*, *numero telefonico* che identificano direttamente Mario Rossi. Gli insieme di dati personali sono 2 (due): b) e d). Se un trattamento di anonimato rimuove l'insieme d) dei dati personali identificativi ma mantiene - a livello di evento, l'insieme b) nella sua originalità, le informazioni di quest'ultimo permangono personali (identificabili) - per chiunque (titolare o terzi) ne abbia accesso, anche se "disconnesse" dall'insieme d). Le informazioni dell'insieme b) possono considerarsi *anonime,* se utilizzate informa anonima, quindi se statisticamente processate a livello di evento superiore e, ad esempio, rilasciate in forma aggregata: il lunedì il numero di accessi è doppio rispetto al martedì; oppure il pomeriggio rispetto alla mattina. Oppure se sottoposte a funzioni di *anonimizzazione* descritte al paragrafo 2.1.2.

Sull'anonimato, ed in particolare sul requisito di irreversibilità, si può registrare inoltre una sostanziale convergenza di definizione tra le norme internazionali di carattere tecnico (ISO 29100) e quelle di carattere giuridico – alle quali oltre a quelle premesse concorre anche la direttiva relativa alla vita privata e alle comunicazioni (Direttiva 2002/58/CE) per quanto declarato al considerando 26) e disciplinato ai successivi art. 6 comma 1, art. 9 comma 1[198];

---

[196] In argomento si indica: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI , *Relazione anno 2014*, pag. 48-49.

[197] L'esempio citato è configurabile anche nel territorio comunitario, benché WhatsApp Inc sia assimilabile ad un titolare del trattamento non stabilito nell'Unione, in ragione del principio di territorialità di cui al GDPR, art. 3 *Ambito di applicazione territoriale*, comma 2): *il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

[198] DIRETTIVA 2002/58/CE, considerando 26): *I dati relativi al traffico utilizzati per la commercializzazione dei servizi di comunicazione o per la fornitura di servizi a valore aggiunto dovrebbero inoltre essere cancellati o resi anonimi dopo che il servizio è stato fornito;*
art. 6, comma 1: *I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1*
art. 9, comma 1: *Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di*

direttiva che si rivela significativa per la l'equivalenza che pone tra le operazioni di *anonimizzazione* (nell'assunto che sia permanente) e quelle di cancellazione di dati personali quando ritenuti non più necessari per la finalizzazione di predefiniti scopi di utilizzo. In argomento lo standard ISO 29100:2011 (*Information technology -- Security techniques -- Privacy framework*) definisce l'*anonimizzazione*[199] come processo nel quale le informazioni personali identificabili (*PII, Personal Identifiable Information*) sono modificate irreversibilmente in modo tale che un titolare di *PII* non possa più essere identificato direttamente o indirettamente, né dal singolo responsabile del trattamento di *PII* né dallo stesso in collaborazione con altri.

Di seguito - anche attraverso la disamina delle principali tecniche di *anonimizzazione*, viene illustrato come l'irreversibilità sia una caratteristica contestuale e relativa e come le informazioni personali rese anonime possono ugualmente concorrere a definire ed arricchire i profili personali delle persone innescando, quindi, processi di re-identificazione e ponendo nuovamente problemi di protezione delle informazioni personali.

2.1.1. ANALISI TECNICO-GIURIDICA DEL TRATTAMENTO DI *ANONIMIZZAZIONE.*

Gli elementi contestuali che concorrono alla modellazione di un trattamento di *anonimizzazione* e che ne configurano efficacia, affidabilità e robustezza rispetto alla possibile re-identificazione attengono sia l'analisi tecnica (2) sia quella giuridica (1) per le implicazioni di tutela del trattamento e dell'interessato. Quanto a quest'ultimo aspetto è possibile distinguere due diversi livelli a seconda che si consideri l'*anonimizzazione* – essa stessa, come trattamento successivo che persegue l'ulteriore finalità di impedire la re-identificazione del soggetto interessato con ogni mezzo ragionevole (1.a) oppure come strumento volto a garantire il mantenimento della liceità di un generico e iniziale trattamento (1.b):

1.a) Nel primo caso l'*anonimizzazione* risponde alle condizioni che definiscono la liceità del trattamento, descritti in dettaglio al precedente capitolo 1, e che attengono in particolare: la *necessarietà* rispetto sia a prerogative del soggetto interessato che del titolare o responsabile del trattamento[200]; la previsione delle tipologie di dati oggetto di

comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto.

[199] ISO 29100:2011, Terms and Definitions, 2.2 anonymization: *process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party*

[200] GDPR, art. 6, *Liceità del trattamento* comma 1) lettere b)-f)

anonimizzazione, i soggetti ai quali possono essere comunicati e i periodi di conservazione; le finalità del processo di *anominizzazione* e la relativa limitazione in caso di differenziazione in particolare per quanto attiene[201]: il nesso tra le finalità per le quali sono stati (originariamente) raccolti i dati personali e le finalità della loro *anonimizzazione*; il contesto di originale raccolta e le *ragionevoli* aspettative delle persone interessate circa il loro ulteriore impiego; la natura dei dati personali e l'impatto sulle persone interessate; le misure di salvaguardia adottate dal responsabile del trattamento per garantire un trattamento equo e per prevenire ripercussioni indesiderate sulle persone interessate. Ciò nel presupposto che siano verificati alcuni prerequisiti di qualità dei dati[202], ovvero che nei confronti dell'interessato in particolare non sia pregiudicata la correttezza e l'esattezza dei dati *anonimizzati*; e che risultino mantenuti l'adeguatezza, la pertinenza e la minimizzazione originarie.

1.b) Nel secondo caso, l'*anonimizzazione* (se si considerano orientamento e disposizioni del CODICE) o la *pseudonimizzazione* (se si considerano quelle del GDPR) sono processi che rafforzano - seppur con intensità sostanzialmente diverse, i prerequisiti di qualità[203] - la minimizzazione dei dati, e di sicurezza; la liceità del trattamento ed i diritti dell'interessato con particolare riferimento alla prerogativa del soggetto interessato di richiedere la trasformazione in forma anonima (sovrapponibile ad una cancellazione) dei dati personali trattati in violazione della legge, se la conservazione non è necessaria in relazione alle finalità di iniziale raccolta e trattamento[204] oppure per vincolare la

---

[201] GDPR, art. 6, *Liceità del trattamento* comma 4) lettere a)-d).
Inoltre in argomento si indica: a) il parere Working Party ex art. 29 n. 203 - Opinion 03/2013 *on Purpose Limitation* 02 Aprile 2013 pag. 3; 21-27

[202] GDPR, art. 5, *Principi applicabili al trattamento dei dati personali* comma 1) lettere a)-f)

[203] CODICE, Art. 3. Principio di necessità nel trattamento dei dati, comma 1: *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.*
GDPR, art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*, comma 1) T*enendo 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.*
Art. 89 *Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici* comma1) *Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.*

[204] CODICE, art. 7 Diritto di accesso ai dati personali e altri diritti, comma 3): *L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in form anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) sono state portate a conoscenza, anche per*

diffusione di particolari dati (ad esempio attinenti indagini, ispezioni, prestazioni professionali; dati sanitari; dati sensibili; informazioni di traffico e ubicazione nell'ambito delle comunicazioni)[205].

Benché il regolamento articoli solo la *pseudonimizzazione*, la configurazione tecnica delle tecniche di *anonimizzazione* è ben sintetizzata nel considerando 26) del GDPR, che in un certo senso configura il dato anonimo speculare al dato personale: "*...Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici....*".

Ai fini dell'analisi tecnica dell'anonimato occorre quindi considerare che:

2.a) i dati *anonimizzati*, sono dati che permangono attinenti ad un soggetto interessato ma che non ne consentono (più) l'identificazione[206];

2.b) impossibilità di re-identificazione e mezzi tecnologici utilizzabili risultano interdipendenti in termini di "*ragionevolezza"*, entrambi vanno contestualizzati alle circostanze specifiche: elencare, quindi, casi di efficace *anonimizzazione* risulta non solo impossibile, ma anche inutile o anacronistica perché le conclusioni ricavate potrebbero essere rapidamente superate dalla sempre crescente potenzialità di collegamento incrociato e trasversale, che tecniche di *data mining* consentono di effettuare tra: i diversi *repositories* di dati personali, le molteplici fonti e l'esponenziale disponibilità di informazioni personali rilasciate sul web[207].

---

quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
GDPR, considerando 28) *L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.*
considerando 29) *Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento.*

[205] CODICE, art.22 *Principi applicabili al trattamento di dati sensibili e giudiziari*
Titolo VIII *Lavoro e previdenza sociale*, art.112 *Finalità di rilevante interesse pubblico*
Titolo X *Comunicazioni elettroniche*, art. 123 *Dati relativi al traffico*; art. 126 *Dati relativi all'ubicazione*

[206] In argomento si indica il parere Working Party ex art. 29 n. 136 - Opinion 4/2007 *on the concept of personal data*, 20 Giugno 2007 pag. 21.

[207] In argomento, sugli aspetti di Privacy Preserving connesso alle tecniche di Data Mining si rimanda la consultazione delle motivazioni introduttive descritte negli abstract dei seguenti contributi:

All'analisi tecnica dell'efficacia dell'anonimato concorrono:

1. la dinamicità delle tecnologie, delle competenze di tutti gli attori coinvolti (non a caso la norma su questo aspetto contempla non solo il titolare del trattamento ma anche i terzi coinvolti o destinatari delle informazioni *anonimizzate*) e soprattutto dei costi di *anonimizzazione* correnti (*ragionevolmente* sostenibili), misurati con quelli prevedibili tenendo conto della crescente disponibilità di mezzi tecnici a basso costo per identificare le persone nelle banche dati, all'accessibilità pubblica sempre maggiore, ad esempio in materia di *Open Data*, e ai numerosi esempi di *pseudonimizzazione* o *anonimizzazione* incompleta[208];
2. gli interventi sull'insieme di dati (anche privati) attinenti attività e comportamenti dell'interessato, da considerarsi complementari all'eliminazione dei dati personali identificativi volti a ridurre la probabilità di deduzione, correlazione e collegamento;
3. considerare – in maniera circostanziata e contestuale, il mantenimento dei requisiti di cui ai precedenti due punti anche quando i dati (ritenuti ragionevolmente *anonimizzati* e quindi in teoria non soggetti alla disciplina di protezione dei dati personali) sono rilasciati ad altri titolari o responsabili del trattamento per il perseguimento di proprie e diverse finalità;
4. evitare di sottostimare i rischi connessi dal considerare i dati *pseudoanonimizzati* equivalenti ai dati anonimi[209]: come verrà meglio precisato nel successivo paragrafo 2.1.3 *La Pseudonimizzazione* questa agisce sul dato identificativo e non sulla relazione di attribuzione (dato_identificativo, persona) come invece accade nel trattamento di *anonimzzazione*;
5. nonché evitare di sottostimare i rischi derivanti dalla "scopertura regolatoria" (in materia di protezione dati personali) su dati anonimi che, in quanto informazioni generiche, per un verso potrebbero essere oggetto di altri atti regolatori (ad esempio della direttiva 2002/58/CE) e per un altro verso impattare le legittime aspettative o le scelte delle persone concorrendo, per esempio, alla definizione di profili o alla configurazione di decisioni da parte del responsabile del trattamento che potrebbero

PRESSWALA FRENY, THAKKAR AMIT, BHATT NIRAV, *Survey on Anonymization in Privacy Preserving Data Mining,* International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015 (2015)
SASHIREKHA K., SABARISH B.A., SELVARAJ AROCKIA, *A Study on Privacy Preserving Data Mining*, International Journal of Innovative Research in Computerand Communication Engineering Vol. 2, Special Issue 3, July 2014 (2014)

[208] In argomento si riporta: http://www.ilpost.it/2011/06/22/anonimato-online/, *L'anonimato online non è più quello di un tempo*, Il New York Times riflette sulla facilità di identificazione offerta oggi dalla rete, e sostiene che non sia male

[209] In argomento si indica il parere Working Party ex art. 29 n. 136 - Opinion 4/2007 *on the concept of personal data*, 20 Giugno 2007 pag. 18-20.

produrre (sebbene indirettamente) effetti sulle persone in contrasto con il principio di *limitazione della finalità* (GDPR, art. 5 *Principi applicabili al trattamento dei dati personali*, comma 1) lettera b)). Si ritiene utile richiamare che in base a tale principio, le aspettative legittime delle persone interessate in merito a trattamenti successivi dei loro dati vanno valutate alla luce dei fattori contestuali rilevanti, quali la natura del rapporto tra le persone interessate e i responsabili del trattamento, gli obblighi normativi applicabili e la trasparenza dei trattamenti dei dati;

6. considerare che le tecniche di *anonimizzazione* e *pseudonimizzazione* puntano rompere o indebolire il riferimento associativo alla persona ma dovrebbero poter mantenere - senza variarne la correttezza, la finalità di successive analisi aggregate e la (ri) utilizzabilità complessiva dei dati di trattamento e, per quanto possibile, la semantica. Ad esempio se i dati di trattamento attengono (tra l'altro) informazioni sugli accessi ad un servizio (come nell'esempio riportato al paragrafo 2.1) questi dopo l'*anonimizzazione* dovrebbero poter continuare ad essere utilizzabili, ad esempio, per valutazioni statistiche (es. media degli accessi), monitoraggio o rilevazioni di anomalie (es. scopertura del servizio);

7. valutare l'affidabilità e l'efficacia delle tecniche di *anonimizzazione* rispetto a proprietà intrinseche delle informazioni, che nel contesto della re-identificazione originano forme di rischio e relativi attacchi sull' insieme di dati resi anonimi o *pseudonimi;* in tal senso si distinguono:

   (a) l'*individuazione*, che corrisponde alla possibilità di isolare alcuni o tutti i dati che identificano una persona all'interno dell'insieme di dati; l'unicità del dato esaminato favorisce questo tipo di proprietà;

   (b) la *correlabilità*, che corrisponde alla possibilità di correlare almeno due dati concernenti la medesima persona interessata o un gruppo di persone interessate (nella medesima banca dati o in due diverse banche dati);

   (c) la *deduzione*, che – nell'ipotesi di rappresentare le informazioni tramite la coppia (attributo, valore), corrisponde alla possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi.

Formulate queste premesse, l'anonimato deve essere considerato un processo di trattamento tutt'altro che *una-tantum* e mantenibile nel tempo, con un intrinseca probabilità di

re-identificazione favorita in contesti informazionali ad elevato e massivo scambio di informazioni (*Big Data, IoT, Internet of Things*) fortemente interconnesse e collegabili a costi sempre minori (ad esempio in *cloud computing*) e - come tali, incompatibili con il principio di minimizzazione dei dati, presupposto intrinseco e strutturale dell'anonimato.

L'anonimato quindi dovrebbe essere considerato come un trattamento soggetto a periodica revisione sul mantenimento nel tempo della *ragionevolezza* dei mezzi e delle risorse utilizzabili; ciò in ragione della sempre più facile interconnessione dei dati, consentita dalle *disruptive technologies* che nel loro insieme favoriscono il reperimento di informazioni ausiliarie riferibili alla persona a cui collegare il dato *anonimizzato* e, non secondariamente, del collegamento alle caratteristiche distintive fisiche della persona implementato dalle *Big Speech Data tecnologies*[210]; fattori, questi, che rendono l'anonimato un processo meno assoluto[211].

Rappresentate queste osservazioni, pur nella consapevolezza di come – sull'argomento, le prescrizioni del GDPR abbiano reso quelle del CODICE, in un certo senso, anacronistiche al contesto di tecnologia e comunicazione attuale e che per quanto lungimiranti risultano comprensibilmente logorate da un trascorso tecnologico di 14 anni, si ritiene sia utile che necessario mantenere a riferimento il trattamento e la funzione dell'anonimato declarati nel CODICE all'art. 4 comma 1, lettera n) sulla definizione di *dato anonimo* e all'art. 3 *Sul principio di necessità del trattamento dei dati.*

Ciò per tutelare il diritto all'anonimato di una persona laddove l'insieme dei fattori obiettivi che concorrono a valutare la ragionevolezza e la sostenibilità dei mezzi (tecnologie) e risorse (tempi, costi e competenze) utilizzabili - seppur lungo un definito intervallo di tempo, ne sostengono l'efficacia e la irreversibilità della *de-identificazione,* finalità questa che configura l'anonimato oltre che come trattamento successivo anche come tutela integrata nei trattamenti e come vera e propria misura di *privacy* Su tale riflessione si rimanda al paragrafo conclusivo 2.1.4 - *Il diritto all'anonimato: profilo e identificabilità della persona.*

---

[210] https://www.slideshare.net/enrdenti/privacy-through-anonymisation-in-largescale-sociotechnical-systems-multilingual-contact-centres-across-the-eu, *Privacy through anonymisation in large scale socio-technical systems,* Cevenini C., Denti E., Omicini A., Cerno I., INSCI 2016

[211] In argomento si indica: Morelato E., *Anonimato e Protezione dei dati personali*, in Giusella Finocchiaro (a cura di), "Diritto all'anonimato, Anonimato, nome e identità personale", CEDAM, 2008, p. 205-212.
Ed inoltre: http://www.ilpost.it/2011/04/28/il-declino-dellanonimato-online/ *Il declino dell'anonimato online*, Arriva Facebook a gestire i commenti e le registrazioni degli utenti, e molti siti non vedevano l'ora Per Mark Zuckerberg l'anonimato "è un esempio di mancanza di coerenza"

2.1.2. LE TECNICHE DI *ANONIMIZZAZIONE.*

Di seguito sono illustrate le principali tecniche di *anonimizzazione* secondo un analisi compariva tratta dal parere Working Party ex art. 29 n. 216 - Opinion 05/2014 *on Anonymisation Techniques* del 10 Aprile 2014, che - fissati i mezzi tecnologici concorrenti sia in fase di *anonimizzazion*e che *re-idendentificazione* e ragionevolmente utilizzabili per grado di sviluppo e disponibilità, ne evidenzia la capacità di prevenire i rischi o contrastare gli attacchi di *individuazione*, *correlazione* e *deduzione*; sono brevemente indicati i punti di forza – quindi garanzie e grado efficacia, e di debolezza – quindi vulnerabilità e insuccesso, impatto e ulteriori rischi per l'interessato. Il dominio delle funzioni di *anonimizzazione* è composto dai dati di trattamento originale rappresentanti, ad esempio, comportamento, attività o caratteristiche del soggetto interessato (includenti informazioni personali, private o anche sensibili)[212]. Nella figura proposta al paragrafo 2.1. si tratta delle informazioni contenute, tipicamente, nel livello intermedio o più esterno.

Le tecniche di *anonimizzazione* si distinguono in due categorie: *randomizzazione* e *generalizzazione,* entrambe puntano a rompere (o indebolire) il legame associativo tra i quasi-identificatori e gli attributi privati, introducendo nell'insieme di dati trattati un certo grado di incertezza (probabilistica) sull'attribuzione di un dato *anonimizzato* ad un soggetto interessato.

Nessuna delle due tecniche è esente da carenze: fissato il contesto informazionale, la tipologia di dati, i dispositivi e i soggetti interessati, alla più ottimale strategia di *anonimizzazione* concorrono funzioni diverse a maggior garanzia del mantenimento della de-identificazione. In generale tutte le tecniche sono precedute dalla eliminazione degli *attributi ovvi* o dei *quasi-identificatori.* Teoricamente - ad *anonimizzazione* avvenuta, dovrebbero essere mantenute distribuzione statistica complessiva, gamma di valori possibili, rendendo statisticamente uguali i valori aggregati indipendentemente se calcolati sui valori veri o randomizzati[213].

Sul rispetto di quest'ultimo requisito si misurano efficacia e vulnerabilità delle varie funzioni, come sintetizzato nelle seguenti tabelle 3.1. e 3.2.

---

[212] Si assume che tali dati possano essere rappresentati in modalità tabellare nella forma (attibuto_di_trattamento, valore_immesso); i quasi-identificatori sono combinazioni qualsiasi di caratteristiche della persona utili ad identificarla; se l'identificazione è diretta i quasi-identificatori coincidono con i dati identificativi ai sensi dell'art. 4 comma 1) lettera n) del CODICE, ad esempio risulta un quasi-identificatore la combinazione (nome, cognome, data di nascita). In generale i dati da voler proteggere tramite anonimato sono quelli relativi agli attributi privati che tramite i quasi-identificatori e a loro volta tramite gli identificatori identificano il soggetto. Ad esempio nella combinazione (nome, cognome, codice fiscale, stipendo annuo) i primi 3 attributi formano un identificatore che identifica direttamente la persona e al contempo la associa al quarto attributo privato.

[213] Ad esempio se in un insieme di dati gli attributi privati attengono dati economici di una persona (stipendio annuo) l'*anonimizzazione* punta a scollegare questo dato dai dati identificativi la persona, ma dovrebbe essere mantenuta – senza variarne la correttezza e l'effettiva utilizzabilità, la finalità (ad esempio) di poter effettuare analisi statistiche sia aggregate (es. calcolo della media) sia *longitudinali* incrociando (in maniera invisibile) gli attributi privati con i quasi-identificatori (es. la media per fasce di età).

La ***randomizzazione*** raggruppa funzioni di *anonimizzazione* che falsano i dati riducendone la veridicità, puntano ad eliminare (o meglio attenuare) il legame associativo puntuale con la persona a cui si riferiscono, introducendo informazione pseudocasuale (rumore) o disordine nell'insieme di dati. In questo gruppo si distinguono:

(1) **la permutazione –** consiste nel mescolare casualmente i *valori_immessi* relativi ai dati di trattamento da *anonimizzare* permutandoli e disaccoppiandoli; l'attributo pur rimanendo invariato nel suo *valore_immesso* viene associato ad un diverso soggetto scelto a caso;

(2) **il rumore statistico** – consiste nell'aggiungere informazione aleatoria ai *valori_immessi* perturbandoli e rendendoli meno accurati;

(3) **la privacy differenziale** – consiste nell'affiancare ad un insieme di dati statistico[214] un altro insieme che differisce dal primo al più per un solo elemento, tale che le risposte alla stessa interrogazione su entrambi siano indistinguibili con probabilità prossima a 1. Se ciò accade la probabilità di dedurre informazioni sull'unico individuo differente è prossima allo 0. Il secondo insieme viene costruito aggiungendo rumore statistico. Dovendo mantenere il primo insieme di dati, la privacy differenziale è considerabile una tecnica di *pseudonimizzazione*;

(4) Un'ulteriore tecnica di *anonimizzazion*e per randomizzazione è quella dei **questionari deliberati** – che consiste nel contrastare la polarizzazione (cioè l'errore sistematico) dei questionari statistici[215], anch'essi come nel caso della privacy differenziale presuppongono indagini con risposte aggregate e non specifiche. La tecnica del *questionario deliberato* consiste nella randomizzazione delle possibili risposte raggruppate a priori in categorie tale da consentire al soggetto di collocare correttamente la propria risposta senza percepire intrusioni per la propria riservatezza, e a chi somministra il questionario di sconoscere in quale gruppo ricade la risposta.

[214] Gli insiemi di dati statistici (o base di dati statistici) sono insiemi ai quali si accede per interrogazioni aggregate riguardanti gruppi di persone e non solo un individuo. Benché questi insiemi di dati non consentano interrogazioni specifiche, sotto certe condizioni è possibile risalire al singolo individuo

[215] Il questionario polarizzato è una rilevazione statistica verso la quale la risposta viene omessa o falsata dalla persona che ritiene minata la propria privacy.

		Punti di Forza *Garanzie/Efficacia*	Punti di Debolezza *Vulnerabilità/Insuccesso*	Impatto per l'interessato
Randomizzazione	**Permutazione**	Invarianza di distribuzione statistica e gamma di valori complessive. Riduce l'individuazione perché i dati sono (presi singolarmente) più incerti e meno affidabili. Riduce la deduzione perché variata la distribuzione dei *valori_immessi.*	Erronea scelta del *valore_immesso.* Inefficacia della casualità della permutazione. Analisi longitudinali (tra quasi-identificatori e attributi) falsate. Rottura del legame logico e di correlabilità tra i quasi-identificatori e gli attributi privati tremite corrispondenze poco plausibili, con conseguente: Possibile riparazione del dato anonimizzato e ricostruzione della vera associazione tra gli attributi privati e gli identificatori (persone). Debole rispetto alla correlabilità.	Associazione di un dato vero ad un'altra persona
	Rumore statistico	I dati rumorosi riducono la probabilità di deduzione, di individuazione (seppur meno efficace rispetto alla permutazione) di correlazione (rivelandosi più efficace rispetto alla permutazione).	Scelta del rumore. Equilibrio tra l'aggiunta di rumore, accuratezza dell'informazione originale e la sua utilizzabilità Mantenimento dell'invarianza di distribuzione statistica e gamma di valori complessive. Individuazione della persona mediando le risposte su molteplici interrogazioni. Produce falsi positivi o negativi. Il rumore può essere incoerente (fuori scala) o invariante Espone la possibilità di riparare i dati o risalire al criterio di rumore.	L'attribuzione rumorosa potrebbe esporre l'interssato ad un rischio imprevisto maggiore di quella corretta.
	Privacy Differenziale	In caso di statistiche aggregate è sensibilmente ridotto il rischio di individuazione, con maggiore efficacia rispetto alle precedenti funzioni.	Scelta e sufficienza del rumore. Correlazione e deduzione della persona mediando le risposte su molteplici interrogazioni.	Quello tipico delle funzioni di *pseudonimizzazione*

Tabella 3.1 - Valutazione comparativa delle tecniche di *anonimizzazione* per randomizzazione

La ***generalizzazione*** raggruppa funzioni di *anonimizzazione* che rendono meno dettagliati gli attributi di un soggetto, generalizzandoli e diluendoli, modificandone l'ordine di grandezza e riducendo il livello di dettaglio. La non individuabilità della persona si basa sull'aumento dei potenziali interessati riferibili a un certo attributo. Ne discende che più combinazioni di dati presentino gli stessi attributi generalizzati (per esempio il prefisso telefonico, se la funzione ha generalizzato da numero telefonico a prefisso; oppure la regione se ha generalizzato da provincia a regione); l'insieme di queste combinazioni prende il nome di classe di equivalenza maggiore è la cardinalità della classe tanto più bassa è la probabilità di re-identificare un soggetto che vi appartiene (e che condivide con gli altri soggetti medesimi valori generalizzati), quindi di collegarlo al corrispondente attributo privato. In questo gruppo di distinguono:

(1) **l'aggregazione e k-anonimato** – generalizza l'insieme di dati originario definendo classi di equivalenza tutte di cardinalità pari o superiore a un prefissato valore (k).

(2) ***L-L*-diversità/*T*-vicinanza** – è un'estensione del k-anonimato che punta a ridurre i rischi di deduzione, facendo in modo che in ciascuna classe di equivalenza ogni attributo abbia almeno *L* valori diversi (*L-L-Diversità*) e quanto più vicini alla distribuzione iniziale (*T-vicinanza*).

		Punti di Forza *Garanzie/Efficacia*	**Punti di Debolezza** *Vulnerabilità/Insuccesso*	**Impatto per l'interessato**
Generalizzazione	**Aggregazione e *k*-anonimato**	Robusto alla individuazione, l'appartenenza di un soggetto alla medesima classe di equivalenza di cardinalità *k* ne aumenta l' indistinguibilità dagli altri *k-1* soggetti. Riduce la correlabilità.	Scelta della cardinalità *k*, con presenza di classi con scarsa variabilità di attributi. Scelta dei quasi-identificatori da generalizzare. Debole rispetto alla deduzione: se si deduce a quale classe appartiene il soggetto, è abbastanza facile recuperare la chiave di generalizzazione.	Deduzione di dati personali privati o sensibili.
	L-L-diversità/T-Vicinanza	Robusto alla individuazione, l'appartenenza di un soggetto alla medesima classe di equivalenza di cardinalità *k* ne aumenta l' indistinguibilità dagli altri *k-1* soggetti. Riduce la correlabilità. Robusto alla deduzione.	Scelta della cardinalità *k*, con presenza di classi con scarsa variabilità di attributi. Scelta di *L* e di *T*.	Deduzione di dati personali privati o sensibili.

Tabella 3.2 - Valutazione comparativa delle tecniche di *anonimizzazione* per generalizzazione

La sfida di tutte le funzioni di *anonimizzazione* è quella di trovare la miglior calibratura tra il modificare gli attributi *veri* di un insieme di dati personali per proteggere la sfera privata di una persona e al contempo mantenerne la valenza semantica e descrittiva, l'utilità del dato di trattamento rispetto alle predefinite finalità, evitando per un verso di rendere i dati inaccurati o inidonei rispetto ad ulteriori analisi; e per un altro verso evitando di introdurre nuovi e non previsti rischi per l'interessato.

2.1.3. LA *PSEUDONIMIZZAZIONE*.

La *pseudominizzazione*[216] è una tecnica di *privacy by design*[217] ed una misura di sicurezza[218]; il GDPR all'art. 25, 32 la ritiene rispettivamente una tutela di trattamento, una garanzia di efficace attuazione dei principi di protezione dei dati e di soddisfacimento dei requisiti del regolamento, contemplandola al contempo (art. 32) come esplicita misura tecnica di sicurezza.

Anch'essa può essere ritenuta un trattamento successivo con la finalità di interrompere il legame associativo che intercorre tra i dati personali e il soggetto interessato senza tuttavia romperlo come accade per il trattamento e le tecniche di *anonimizzazione.*

La pseudonimizzaizone è un processo in se reversibile nella misura in cui si dispone di informazioni aggiuntive. Consta nel sostituire i valori di attributo dei dati con altri valori non intellegibili (che comunque si mantengono univoci), solitamente calcolati mediante utilizzo congiunto di più funzioni (o algoritmi) crittografiche sia reversibili che irreversibile, comunque note. La sua efficacia dipende dalla chiave utilizzata e dalla sua gestione; al fine di ridurre i rischi di *individuazione*, *correlabilità* e *deduzione* di dati personali e di associazione con la persona è buona prassi utilizzare: chiavi di cifratura diverse per diversi sistemi di dati; chiavi diverse per diversi soggetti e separare la conservazione della chiave rispetto agli pseudonimi.

Se disponendo di informazioni aggiuntive o, in assenza di queste, avvalendosi di tutti i mezzi e risorse *ragionevolmente* utilizzabili, il dato pseudonimo viene *rotto* (decodificato) allora il collegamento dei dati di trattamento con la persona viene ripristinato nella propria originale certezza, a differenza dell'*anonimizzazione* che punta a introdurre incertezza nella attribuzione *dato<=>persona.*

In tal senso mentre l'anonimizzazione incidendo specificatamente sulla semantica della relazione di identificabilità tra i dati personali e il soggetto interessato può essere considerata una vera e propria misura di privacy, la pseudonimizzazione incidendo specificatamente sui

---

[216] GDPR all'art.4 Definizioni comma 5 *pseudonimizzazione:: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*

[217] GDPR art. 25 P*rotezione dei dati fin dalla progettazione e protezione per impostazione predefinita* comma 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.*

[218] GDPR art. 32 *Sicurezza del trattamento* comma 1) lettera a) *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;*

dati identificativi può essere considerata come una misura di sicurezza.

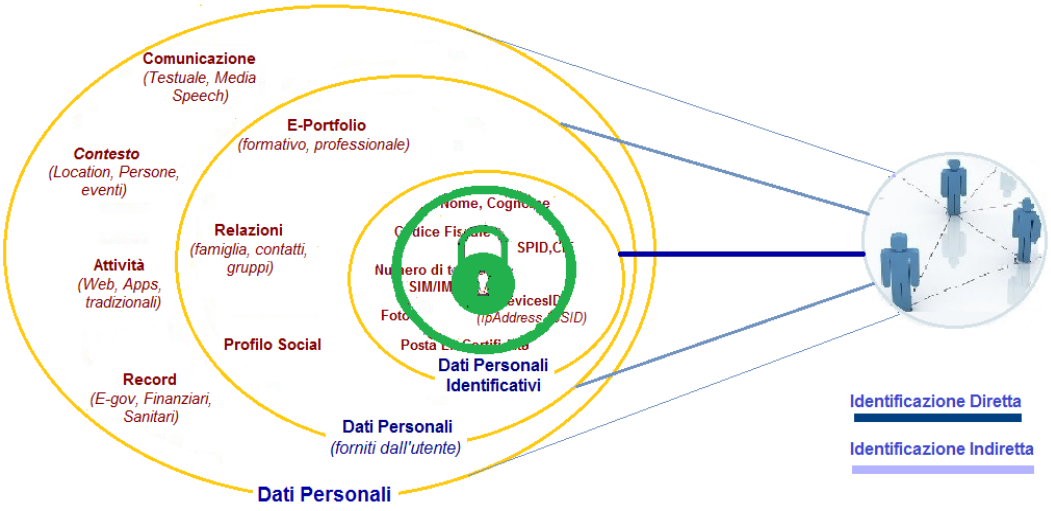


Figura 3.2 - Trattamento di *pseudonimizzazione*

La *pseudonimizzazione* non interviene e non altera l'associazione (logica) biunivoca di identificazione/identificabilità *dato*<=>*persona* ma prevalentemnte agice sui dati identificativi rendendo molto complessa l'identificazione, al imite impossibile senza l'utilizzo di informazioni aggiuntive.

La *pseudonimizzazione* si rivela una debole contromisura ai rischi di *individuazione*, *correlabilità* e *deduzione*. Il risultato della funzione di *pseudonimizzazione* cambia il valore degli attributi ma ne lascia invariata l'unicità, rendendo il soggetto individuabile da un attributo unico, in analogia e nella stessa misura dell'insieme originale.

Anche la correlabilità non varia rispetto all'insieme originale, essendo di semplice computazione tra i dati che utilizzano lo stesso attributo *pseudonimizzato;* solo nel caso in cui nessun altro attributo contenuto nell'insieme di dati originali possa essere utilizzato per identificare il soggetto interessato e se è stato eliminato ogni legame tra l'attributo *originario* e quello *pseudominizzato,* non risulta sussistere alcun riferimento incrociato ovvio tra due insiemi di dati che utilizzano attributi *pseudonimizzati* diversi. Analogamente, la *deduzione* è fattibile in insiemi di dati che utilizzano lo stesso attributo *pseudonimizzati* per una persona o se gli pseudonimi sono molto evidenti e non mascherano sufficientemente l'identità originale della persona.

I dati pseudonimi *potrebbero essere ancora essere attribuiti ad una persona fisica mediante l'utilizzo di ulteriori informazioni*[219], permanendo quindi (a differenza della *anonimizzazione*) soggetti alle prescrizioni del regolamento e alle relative tutele.

[219] Cfr GDPR all'art.4 Definizioni comma 5)

La sua applicabilità è strettamente commessa al principio di finalità nel senso che non può ostacolarne o comprometterne il raggiungimento e non può essere applicata indiscriminatamente e con medesime modalità a tutti i trattamenti.

2.1.4. IL DIRITTO ALL'ANONIMATO: PROFILO E IDENTIFICABILITÀ DELLA PERSONA.

Se si analizza preliminarmente il concetto di anonimato, occorre rilevare l'assenza di una definizione normativa[220]; al di fuori del contesto di trattamento e gestione digitale delle informazioni personali in effetti l'importanza definitoria appariva superflua e superabile assumendo come anonimo ciò che è privo di nome o ciò (un fatto, un evento) che non è riconducibile ad un soggetto. La definizione di dato anonimo inserita nel CODICE[221] anticipa la sempre maggiore importanza della *riconducibilità* e ne coglie quella che oggi è una obbligatorietà di definizione, considerando che pur in assenza di nome la presenza di molte altre informazioni, di sempre più facile e imprevedibile collegabilità, aumentano l'identificabilità della persona cui tali informazioni si riferiscono[222].

Internet e le nuove tecnologie, quindi, ampliano la relatività dell'anonimato (ampiamente disaminata nei precedenti paragrafi) confermandone anche la sua funzionalità alla tutela di altri diritti, atteso che l'anonimato - a differenza del diritto al nome e all'identità riconosciuti e configurati come diritti della personalità, non trova (a tutt'oggi) formale riconoscimento nell'ordinamento giuridico italiano, almeno in via generale e fatta eccezione per quanto previsto nella recente *Dichiarazione dei Diritti in Internet*[223] (2015).

Il diritto all'anonimato, sin dalla sua la prima trattazione strutturata[224] - laddove non negato o considerato un fatto indipendente e ininfluente per il diritto, è stato introdotto e declinato strumentalmente alla tutela di altri diritti, normato e riconosciuto se inserito in

---

[220] In argomento si indica: Morelato E., *Anonimato e Protezione dei dati personali*, in Giusella Finocchiaro (a cura di), "Diritto all'anonimato, Anonimato, nome e identità personale", CEDAM, 2008, p. 12-20

[221] CODICE, Art. 4 - Definizioni, comma 1, lettera n): "*dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;*

[222] Dato anonimo e dato personale possono quindi essere ritenute due facce della stessa medaglia, quella della *attribuzione* e della *riferibilità identificativa*, da intendersi - per quanto illustrato nei precedenti paragrafi relativa e contestuale; inoltre misurabile - in entrambe le direzioni - quella della identificazione (dato personale) e della non re-identificazione (dato anonimo), secondo il parametro della *ragionevolezza*; criterio che rende l'anonimato un concetto non assoluto sia sotto il profilo strettamente tecnico sia per le implicazioni sulle persone interessate e quindi per la declinazione dello stesso diritto all'anonimato, anch'esso relativo e che si configura (riconoscendolo o negandolo) in relazione a determinati soggetti, a circostanze specifiche, e al variare dei casi.

[223] Il nuovo testo della Dichiarazione è stato elaborato dalla Commissione per i diritti e i doveri relativi ad Internet a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015. Il testo è inserito in Appendice

[224] Candian, che in «Anonimato (diritto all')», in *Enc. dir.*, II, Milano, 1958, riconduceva il diritto all'anonimato al diritto alla riservatezza. Tale orientamento tuttavia si rivelò privo di successivi sviluppi e approfondimenti.

alcune leggi speciali.[225]

Con specifico riferimento alla protezione dei dati personali l'anonimato (sia per il Codice che, seppur in misura diversa, per il GDPR) rappresenta tanto una misura estrema per l'esercizio del principio di minimizzazione dell'utilizzo dei dati personali[226]; tanto di controllo, per il soggetto interessato, sulla circolazione delle proprie informazioni attuato con la determinazione limite di oscurarne l'attribuzione, tanto di una nuova e aggiornata forma di riservatezza attuata con la determinazione di escludere gli altri attori dall'identificazione dell'interessato.

Per tutelare la persona (il cittadino digitale) da nuovi rischi, Internet e le nuove tecnologie invocano un riconoscimento del diritto all'anonimato che sia non solo strumentale ma intrinseco. In tale direzione un primo passo è stato compiuto dalla *Dichiarazione dei Diritti in Internet* formulata dalla Commissione parlamentare per i Diritti e i Doveri relativi a Internet che all'art. 10[227] sostiene la protezione dell'anonimato come sostanziale prerequisito ed esercizio di libertà - fissandone comunque limitazioni dettate da superiori tutele per la persona o dal prevalere di rilevanti interessi pubblici. Il permanere del contingente bilanciamento con altri diritti fondamentali, indica il grado di tensione resistente alla configurazione del diritto all'anonimato nella sua autonomia[228].

L'anonimato inteso come determinazione del soggetto, complementa due significativi nuovi diritti di Internet[229] che diversamente risulterebbero svuotati, per esempio, dall'impossibilità di esercitare pienamente il diritto di accesso (o di scelta di quanti e quali dati personali rilasciare); o ancora dalla distorsione dell'intrinseco requisito di neutralità della rete

---

[225] A titolo di esempio, e senza carattere di esaustività, si richiamano le disposizioni in materia di tossicodipendenza in cui l'anonimato si rivela strumentale al perseguimento della finalità di tutelare la salute del paziente; o al dovere previsto in capo al personale sanitario di mantenere anonimi il donatore e il ricevente in caso di trapianti; al diritto della madre di non rivelare la propria identità a tutela della maternità; al diritto dell'autore di rimanere anonimo quale tutela della libertà di espressione. Per un elenco significativo di ulteriori casistiche in cui si ricorre all'utilizzo dell'anonimato o, diversamente, alla sua negazione, si rimanda a: Morelato E., *Anonimato e Protezione dei dati personali*, in Giusella Finocchiaro (a cura di), "Diritto all'anonimato, Anonimato, nome e identità personale", CEDAM, 2008, p. 17-18

[226] CODICE all' Art. 3 comma 1 Principio di necessità nel trattamento dei dati *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.* In una ideale applicazione del principio di necessità la previsione del codice subordina se non esclude il trattamento stesso ogni qual volta sia possibile perseguirne le prefissate finalità attraverso l'utilizzo di dati anonimi

[227] Dichiarazione dei Diritti e dei Doveri in Internet, Art. 10. (*Protezione dell'anonimato*).
1. Ogni persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure. 2. Limitazioni possono essere previste <....>. 3. Nei casi di violazione della dignità e dei diritti fondamentali <...>

[228] In argomento, per una analisi comparativa si indica ZENO-ZENCOVICH V., *Anonymous speech on the Internet,* disponibile alla risorsa http://www.giur.uniroma3.it/materiale/docenti/zeno/materiale/Anonymous%20speech%20(%20in%20Koltay%20ed.).pdf

[229] Cfr Dichiarazione dei Diritti in Internet - art. 2 *Diritto di accesso* e art. 4 *Neutralità della rete.*

esercitabile dal ruolo censorio di intermediari che – in caso di negazione dell'anonimato, condizionerebbero (al limite inibendole) la libertà di pensiero ed espressione introducendo, di fatto, nuove forme di censura.

Un adeguato esercizio del diritto all'anonimato dovrebbe puntare ad abbattere nuovi rischi per la persona riconducibili alla necessità di prevenire possibili diffamazioni in rete o comportamenti socialmente inaccettabili, ma al contempo temperando questa tutela contrastando le implicazione che deriverebbero da un eccesso di esposizione in ragione della attribuzione identificativa delle proprie azioni o delle proprie idee, quali: discriminazione, intimidazione, stigmatizzazione, limitazione della libertà di espressione ed esclusione dai circuiti relazionali.

La resistenza maggiore alla diffusione di idonee pratiche di *anonimizzazione* rimane l'adesione, molto diffusa soprattutto nell'utenza dei *social media,* alle politiche del *real name*[230] che erodono *a-priori* il principio stesso dell'anonimato in forza non tanto di una prassi contrattuale quanto dall'inconsapevolezza di fondo sui reali obiettivi perseguiti da tali tecniche negoziali ovvero di disporre di preziose riserve di dati personali da sfruttare per scopi di *direct marketing* e profilazione, per associare alle persone reali le deduzioni riguardanti attitudini, abitudini, relazioni convergenti in profili molto dettagliati indirizzanti strategie, vantaggi concorrenziali e utili ritorni di mercato.

Il compromesso tra la finalità dichiarata del *real name policy* e la determinazione dell'utente al mantenimento del proprio anonimato può essere raggiunto con il ricorso alle tecniche di *pseudonimizzazione* o con il c.d. *anonimato protetto* che presuppone l'iniziale rilascio delle credenziali identificative a chi garantisce l'accesso in rete ma mantenendo l'utente non identificabile se non, in specifici casi, attraverso l'intervento dell'autorità giudiziaria.

[230] *Real name policy* è la politica attuata in linea di massima da soggetti privati, nonchè da Google Inc. e dai social media di subordinare l'accesso ai servizi offerti all'imposizione unilaterale dell'obbligo di dichiarare i propri dati identificativi. La finalità dichiarata è quella di risalire direttamente agli autori di comportamenti ritenuti non leciti.

3. I SISTEMI DI *PRIVACY POLICIES – PREFERENCES.*

Le regole, le politiche e le relative impostazioni, differenziabili in distinte tipologie e implementate per il tramite di linguaggi e framework costituiscono un sistema che affianca e protegge la gestione del trattamento delle informazioni digitali consentendo di regolamentarne l'accesso e l'utilizzo delle risorse. Nel caso la risorsa è rappresentata da un dato personale, quindi un'informazione in grado di identificare direttamente o indirettamente una persona, le regole concorrono a definire insiemi di politiche di *privacy*.

Le regole di *privacy* intervengono sulle operazioni di trattamento (rilascio delle informazioni, scambio, modifica, archiviazione, cancellazione...) con lo scopo di limitare e controllare le operazioni che gli utenti effettuano, prevenendo azioni accidentali o volute tali da compromettere la correttezza e il legittimo utilizzo dei dati.

Le politiche di controllo dell'utilizzo dei dati personali hanno per *oggetto* la risorsa (dato personale) da proteggere, per *soggetto* le entità che richiedono di poter accedere alla risorsa in genere con un filtro di autenticazione/autorizzazione, per *privilegi* le azioni consentite (o negate) esercitabili dai *soggetti* sugli *oggetti*. La terna (soggetto, oggetto, privilegio) definisce il paradigma di autorizzazione. I *soggetti* possono comprendere: utenti, gruppi, ruoli e processi.

Il controllo dell'accesso è effettuato mediante il meccanismo di controllo dell'accesso, detto anche *reference monitor:* esso intercetta ogni richiesta inviata e stabilisce, tramite l'analisi delle autorizzazioni, se il soggetto richiedente può essere autorizzato (e in quale misura) a compiere l'accesso richiesto. Le politiche per controllo dell'accesso stabiliscono le regole in base alle quali i soggetti possono accedere agli oggetti nel sistema e se e come i diritti d'accesso possono venire trasmessi a terzi; a seconda del criterio utilizzato si distinguono: *politiche discrezionali, politiche mandatorie, politiche basate sui ruoli*[231].

[231] Le *politiche discrezionali* consentono a determinati utenti nel sistema di specificare chi è autorizzato a compiere quali operazioni. Nei sistemi che adottano tale politica, esiste un insieme di autorizzazioni che stabiliscono esplicitamente, per ogni soggetto, i privilegi che questo può esercitare sugli oggetti del sistema. Vengono dette discrezionali in quanto permettono agli utenti di concedere o revocare dei diritti di accesso sugli oggetti, a loro discrezione.
Le politiche mandatorie non consentono agli utenti di modificare lo stato delle autorizzazioni nel sistema; essi possono regolare l'accesso ai dati mediante la definizione di classi di sicurezza, chiamate anche etichette, per i soggetti e gli oggetti del sistema. Le classi di sicurezza sono ordinate parzialmente (o totalmente) da una relazione d'ordine. Il controllo dell'accesso è regolato da una serie di assiomi di sicurezza che stabiliscono la relazione che deve intercorrere fra la classe di un soggetto e quella di un oggetto affinché al primo sia concesso di esercitare un privilegio sul secondo. La relazione che deve essere soddisfatta dipende dal tipo di privilegio considerato. I sistemi che adottano politiche mandatorie sono spesso indicati come sistemi multi-livello.
Le *politiche basate sui ruoli* consentono di assegnare i privilegi non agli utenti ma mediati dal concetto di ruolo, che rappresenta una funzione all'interno di un'azienda. Le autorizzazioni non sono concesse ai singoli utenti ma ai ruoli. Ogni utente è poi abilitato a ricoprire uno o più ruoli ed in questo modo acquisisce le autorizzazioni ad essi associate.
Ulteriori varianti di politiche possono regolare un controllo dell'accesso basato sugli attributi (ABAC Attribute-based Access Control), sulle finalità, sull'accesso temporale, sulla localizzazione.
Cfr http://dawsec.dicom.uninsubria.it/elena.ferrari/wp-content/uploads/2012/10/controlloaccesso1parte.pdf

Le politiche e le relative impostazioni di *privacy (preferences)* possono essere configurate seguendo quattro diversi approcci: *i)* essere definite dal provider tanto nelle regole *(privacy notice)* quanto nelle impostazioni predefinite *(default settings)*; *ii)* essere definite e personalizzate dall'utente; *iii)* con entrambe le precedenti specifiche; oppure *iv)* dinamicamente al variare del comportamento dell'utente, delle sue attitudini o della reputazione segnalata.

3.1. LE PRIVACY POLICIES DI TIPO "PROVIDER CENTERED". ESEMPI.

Le regole di *privacy* sono definite e configurate dal provider del servizio il quale espone all'utente anche un set predefinito di impostazioni base. Un tipico esempio è la definizione dell'informativa privacy (*privacy notice)* di un Social Network o di un'App di messaggistica come WhatsApp, unitamente ai *default settings* predefiniti discriminanti quale e con chi condividere un determinato contenuto (ad esempio il profilo, lo stato, il numero di telefono).

ESEMPIO – INFORMATIVA PRIVACY WHATSAPP[232]

Informativa sulla privacy di WhatsApp
Ultima modifica: 25 Agosto 2016 (versioni archiviate)
Il rispetto per la privacy dei nostri utenti è insito nel nostro DNA. Da quando abbiamo creato WhatsApp, il nostro obiettivo è sempre stato realizzare Servizi con un livello di privacy elevato.

WhatsApp è un fornitore di servizi di messaggistica, chiamate Internet e altre tipologie di servizi per utenti di tutto il mondo. La nostra Informativa sulla privacy illustra le nostre procedure relative alle informazioni (messaggi compresi). Illustriamo ad esempio quali informazioni raccogliamo e la modalità in cui ciò incide sull'utente. Illustriamo inoltre i passaggi adottati per proteggere la privacy dell'utente, ad esempio il fatto che WhatsApp non archivia i messaggi consegnati e fornisce all'utente la possibilità di gestire con chi comunica usando i nostri Servizi.

Con "WhatsApp", "nostro/a/e/i", "noi" o "ci" si intende WhatsApp Inc. La presente Informativa sulla privacy ("Informativa sulla privacy") si applica alle nostre applicazioni, ai nostri servizi, alle nostre funzioni, al nostro software e al nostro sito Web (globalmente i "Servizi"), salvo diversamente specificato.

Si invita a leggere i Termini di servizio di WhatsApp ("Termini"), che illustrano le condizioni applicabili all'uso dei nostri Servizi.

Informazioni raccolte - *WhatsApp riceve o raccoglie informazioni quando rende disponibili e fornisce i propri Servizi, nonché quando l'utente installa, accede o utilizza i Servizi.*

Informazioni fornite dall'utente - I*nformazioni sull'account dell'utente. L'utente fornisce a WhatsApp il proprio numero di cellulare per creare un account WhatsApp. L'utente accetta di fornirci regolarmente i numeri di telefono dei contatti presenti nella rubrica del suo dispositivo mobile, compresi quelli degli utenti dei nostri Servizi e degli altri contatti. L'utente conferma di essere autorizzato a fornirci tali numeri. L'utente può aggiungere altre informazioni al suo account, ad esempio un nome e un'immagine del profilo e un messaggio di stato.*

Messaggi dell'utente. - *WhatsApp non archivia i messaggi dell'utente durante la normale prestazione dei Servizi. Una volta consegnati, i messaggi (compresi chat, foto, video, messaggi vocali, file, e informazioni sulla posizione condivise)*

[232] https://www.whatsapp.com/legal/?l=it#privacy-policy

vengono eliminati dai nostri server. I messaggi dell'utente vengono archiviati sul suo dispositivo. Se non è possibile consegnare immediatamente un messaggio (ad esempio se l'utente è offline), lo archivieremo nei nostri server fino a 30 giorni nel tentativo di consegnarlo. Se dopo 30 giorni il messaggio non è stato ancora consegnato, verrà eliminato. Per migliorare le prestazioni e consegnare i messaggi con contenuti multimediali in modo più efficiente, ad esempio quando molte persone condividono una foto o un video famoso, archivieremo tale contenuto nei nostri server per un periodo più lungo. Offriamo inoltre la crittografia end-to-end per i nostri servizi, che è attiva per impostazione predefinita, quando l'utente e le persone con cui messaggia utilizzano una versione della nostra applicazione rilasciata dopo il 2 Aprile 2016. La crittografia end-to-end significa che i messaggi degli utenti sono criptati per essere protetti dall'essere letti da WhatsApp e da terze parti.

Connessioni dell'utente. - *Per favorire le comunicazioni, creiamo un elenco di contatti preferiti dell'utente, che può creare gruppi e liste broadcast, iscriversi o essere aggiunto ad essi, associandoli alle informazioni del suo account.*

Assistenza clienti. - *L'utente accetta di fornirci informazioni relative all'utilizzo dei nostri Servizi, incluso copie dei messaggi, e alla modalità per contattarlo allo scopo di consentirci di fornirgli assistenza. Ad esempio, l'utente può inviarci un'email contenente informazioni relative alle prestazioni della nostra applicazione o ad altre questioni.*

Informazioni raccolte automaticamente - *Informazioni di uso e di accesso. WhatsApp raccoglie informazioni relative all'utilizzo del Servizio, alla diagnostica e alle prestazioni. Ciò comprende informazioni relative all'attività dell'utente (ad esempio l'utilizzo dei Servizi, la modalità di interazione con terzi tramite i nostri Servizi e simili), file di registro, e registri e report relativi a diagnostica, arresti anomali, sito Web e prestazioni.*

Informazioni sulle operazioni. - *Se l'utente paga per usufruire dei nostri Servizi, WhatsApp potrebbe ricevere informazioni e conferme, ad esempio le ricevute dei pagamenti, comprese quelle provenienti dagli app store o da terzi che elaborano il pagamento.*

Informazioni su dispositivo e connessioni. - *WhatsApp raccoglie informazioni specifiche sul dispositivo quando l'utente installa, accede o utilizza i nostri Servizi. Ciò comprende informazioni quali il modello di hardware, le informazioni sul sistema operativo, le informazioni sul browser, l'indirizzo IP, le informazioni sulla rete mobile, compresi il numero di telefono e gli identificativi del dispositivo. WhatsApp raccoglie informazioni sulla posizione del dispositivo se l'utente usa le funzioni sulla posizione, come quando decide di condividere la sua posizione con i propri contatti, vedere posizioni vicine o quelle che gli altri hanno condiviso con lui, e simili, e a scopi diagnostici e di risoluzione dei problemi ad esempio nel caso in cui l'utente riscontri problemi con le funzioni di posizione dell'applicazione.*
Cookie. - *WhatsApp utilizza i cookie per rendere disponibili e fornire i Servizi, nonché per offrirli sul Web, per migliorare l'esperienza dell'utente, per capire come vengono utilizzati i Servizi e per personalizzarli. Ad esempio, WhatsApp utilizza i cookie per fornire WhatsApp per il web e per il computer e altri servizi basati sul web. WhatsApp potrà pure usare i cookie per individuare le FAQ più popolari e mostrare all'utente contenuti pertinenti relativi ai Servizi. Inoltre, WhatsApp utilizza i cookie anche per ricordare le scelte dell'utente, ad esempio le preferenze relative alla lingua, e per offrire altri contenuti personalizzati sui Servizi. Maggiori informazioni sull'utilizzo dei cookie per la fornitura dei Servizi.*

Informazioni sullo stato. - *WhatsApp raccoglie informazioni sulle modifiche relative all'accesso e allo stato dell'utente nei nostri Servizi, ad esempio la sua presenza online (''stato online''), l'ultima volta che ha utilizzato i Servizi (''ultimo accesso'') e l'ultimo aggiornamento del suo stato.*

Informazioni di terzi - *Informazioni sull'utente fornite da altri utenti. WhatsApp riceve le informazioni fornite da altre persone, che potrebbero comprendere informazioni sull'utente. Ad esempio, quando altri utenti che l'utente conosce utilizzano i nostri Servizi, è possibile che forniscano il suo numero di telefono presente nella rubrica del loro dispositivo (nello stesso modo in cui l'utente può fornire il numero di altri utenti) o che inviino un messaggio all'utente o a gruppi di cui fa parte o che lo contattino telefonicamente.*

Fornitori terzi. - *WhatsApp collabora con fornitori terzi per fornire, migliorare, comprendere, personalizzare,*

commercializzare i propri Servizi e fornire assistenza in relazione ad essi. Ad esempio, collaboriamo con aziende per distribuire le nostre applicazioni, fornire la nostra infrastruttura, la consegna e altri sistemi, offrire informazioni relative a mappe e luoghi, elaborare i pagamenti, comprendere la modalità di utilizzo dei nostri Servizi da parte delle persone e commercializzare i nostri Servizi. In alcuni casi, questi fornitori possono fornirci informazioni sull'utente; ad esempio, gli app store possono fornirci report per la diagnostica e la risoluzione di problemi tecnici.

Servizi di terzi. - *WhatsApp consente l'utilizzo dei Servizi di WhatsApp insieme a servizi di terzi. Se si utilizzano i nostri Servizi insieme a servizi di terzi, potremmo ricevere informazioni sull'utente da tali servizi, ad esempio, in caso di utilizzo del pulsante di condivisione di WhatsApp in un servizio di notizie per condividere un articolo con i contatti, i gruppi o le liste broadcast di WhatsApp nei nostri Servizi oppure in caso di accesso ai nostri Servizi usando la promozione degli stessi dell'operatore di telefonia mobile o del fornitore del dispositivo. Si tenga presente che, utilizzando servizi di terzi, si accettano le condizioni e le informative sulla privacy che ne regolano l'utilizzo.*

Modalità di utilizzo delle informazioni da parte di WhatsApp - *WhatsApp utilizza le informazioni a sua disposizione per rendere disponibili, fornire, migliorare, comprendere, personalizzare, commercializzare i propri Servizi e fornire assistenza in relazione ad essi.*

Servizi di WhatsApp. - *WhatsApp rende disponibili e fornisce i propri Servizi, fornendo al contempo assistenza e migliorando, risolvendo i problemi e personalizzando i Servizi. WhatsApp comprende la modalità di utilizzo dei propri Servizi da parte delle persone e analizza e usa le informazioni a sua disposizione per valutare e migliorare i Servizi stessi, fare ricerche, sviluppare e testare nuovi servizi e funzioni e individuare e risolvere i problemi. Le informazioni dell'utente vengono inoltre utilizzate per fornirgli una risposta quando ci contatta. WhatsApp utilizza i cookie per rendere disponibili, fornire, migliorare, comprendere e personalizzare i Servizi.*

Sicurezza e protezione. - *WhatsApp verifica gli account e le attività e promuove la sicurezza e la protezione all'interno e all'esterno dei Servizi, ad esempio analizzando le attività sospette o le violazioni dei Termini, per assicurare l'utilizzo conforme alla legge dei Servizi.*

Comunicazioni relative ai Servizi e al gruppo di aziende di Facebook. - *WhatsApp comunica con l'utente in merito ai Servizi e alle funzioni, ai Termini e alle informative e ad altri aggiornamenti importanti. WhatsApp potrebbe offrire il marketing per i Servizi e per i servizi del gruppo di società di Facebook di cui fa ora parte.*

Nessun banner pubblicitari di terzi. - *Non consentiamo banner pubblicitari di terzi su WhatsApp. Non abbiamo intenzione di adottarli, ma, se mai lo faremo, aggiorneremo la presente Informativa.*

Messaggi commerciali. - *Consentiremo all'utente e a terzi, come le aziende, di comunicare tra di loro usando WhatsApp, ad esempio tramite informazioni su ordini, transazioni e appuntamenti, notifiche su consegne e spedizioni, aggiornamenti su prodotti e servizi, e marketing. Ad esempio, l'utente potrebbe ricevere informazioni sullo stato dei voli per un viaggio in programma, una ricevuta per un articolo che ha acquistato o una notifica relativa al momento in cui una consegna verrà effettuata. I messaggi che l'utente potrebbe ricevere contenenti marketing potrebbero includere un'offerta per qualcosa che potrebbe interessare. Non vogliamo che l'utente abbia una esperienza simile allo spam; come per tutti i messaggi, l'utente può gestire queste comunicazioni e noi rispetteremo le sue scelte.*

Informazioni condivise tra WhatsApp e l'utente - *Utilizzando e comunicando tramite i nostri Servizi, l'utente condivide le sue informazioni, che a sua volta WhatsApp condivide per rendere disponibili, fornire, migliorare, capire, personalizzare, supportare, e commercializzare i Servizi.*

Informazioni sull'account. - *Il numero di telefono, il nome e l'immagine del profilo, lo stato online e lo stato, l'ultimo accesso e le conferme sono disponibili per tutti gli utenti che utilizzano i nostri Servizi, sebbene l'utente possa configurare le impostazioni dei Servizi per gestire le informazioni disponibili per gli altri utenti.*

Contatti dell'utente e di altri. - *Le altre persone con cui l'utente comunica possono archiviare o condividere a loro*

volta le informazioni (compresi numero di telefono o messaggi) con altre persone all'interno e all'esterno dei Servizi. L'utente può usare le impostazioni dei Servizi e la funzione di blocco all'interno degli stessi per gestire gli utenti dei Servizi con cui comunica e alcune informazioni che condivide.

Fornitori terzi. - *WhatsApp collabora con fornitori terzi per rendere disponibili, fornire, migliorare, comprendere, personalizzare, commercializzare i propri Servizi e fornire assistenza in relazione ad essi. Quando condividiamo informazioni con fornitori terzi, richiediamo che questi utilizzino le informazioni dell'utente in conformità con le nostre istruzioni e le condizioni indicate o con il suo permesso esplicito.*

Servizi di terzi. - *Quando l'utente utilizza servizi di terzi integrati nei nostri Servizi, detti terzi possono ricevere informazioni su ciò che condivide con essi. Ad esempio, se l'utente utilizza un servizio per il backup dei dati integrato nei nostri Servizi (ad esempio iCloud o Google Drive), il servizio in questione riceverà informazioni sui dati condivisi dall'utente. Se l'utente interagisce con un servizio di terzi collegato ai nostri Servizi, fornirà informazioni direttamente a detti terzi. Si tenga cortesemente presente che, utilizzando servizi di terzi, si accettano le condizioni e le informative sulla privacy che ne regolano l'utilizzo.*

Società affiliate- *WhatsApp è entrata a far parte del gruppo di società di Facebook nel 2014. In qualità di membro del gruppo di società di Facebook, WhatsApp riceve informazioni da tale gruppo di società e le condivide con esse. WhatsApp può utilizzare le informazioni che riceve e il gruppo di società può utilizzare le informazioni che WhatsApp condivide con esse per rendere disponibili, fornire, migliorare, comprendere, personalizzare, commercializzare i suoi Servizi e quelli del gruppo di società e fornire assistenza in relazione ad essi. Ciò comprende il miglioramento dell'infrastruttura e dei sistemi di consegna, la comprensione della modalità di utilizzo dei Servizi di WhatsApp o del gruppo di società, la messa in sicurezza dei sistemi e la prevenzione di spam, usi impropri o attività non consentite. Facebook e le altre società del gruppo Facebook possono utilizzare le informazioni di WhatsApp per migliorare le esperienze degli utenti all'interno dei loro servizi come per fornire suggerimenti sul prodotto (ad esempio, suggerimenti relativi ad amici o collegamenti oppure a contenuti interessanti) e per mostrare offerte e inserzioni pertinenti. Tuttavia, i messaggi di WhatsApp dell'utente non saranno condivisi su Facebook per essere visti da altri. Facebook non utilizzerà i messaggi di WhatsApp dell'utente per scopi diversi dall'assistenza a WhatsApp affinché possa rendere disponibili e fornire i Servizi.*

Maggiori informazioni sul gruppo di società di Facebook e sulle procedure sulla privacy sono disponibili nelle relative informative sulla privacy.

Cessione, cambiamento nella compagine societaria di controllo e trasferimento - *Tutti i nostri diritti e obblighi specificati nella presente Informativa sulla privacy possono essere da noi trasferiti liberamente alle nostre società affiliate nell'eventualità di una fusione, acquisizione ristrutturazione o vendita di beni o a mezzo di successione o altra operazione. WhatsApp si riserva inoltre il diritto di trasferire le informazioni dell'utente alle proprie affiliate, a soggetti aventi causa o a un nuovo proprietario.*

Gestione delle informazioni dell'utente - *Se l'utente desidera gestire, modificare, limitare o eliminare le proprie informazioni, può farlo tramite i seguenti strumenti:*

Impostazioni dei Servizi. - *L'utente può modificare le impostazioni dei Servizi per gestire determinate informazioni disponibili agli altri utenti. L'utente può gestire contatti, gruppi e liste broadcast o utilizzare la funzione di blocco per gestire gli utenti con cui comunica.*

Cambio di numero di telefono, nome e immagine del profilo e stato. - *L'utente deve cambiare il numero di telefono utilizzando l'apposita funzione presente nell'applicazione, trasferendo l'account al nuovo numero di telefono. È anche possibile modificare nome, immagine del profilo e stato in qualsiasi momento.*

Eliminazione dell'account WhatsApp. - *L'utente può eliminare l'account WhatsApp in qualsiasi momento (compreso il caso in cui desidera revocare il consenso all'utilizzo delle proprie informazioni da parte di WhatsApp) usando l'apposita funzione presente nell'applicazione. Quando si elimina un account WhatsApp, i messaggi non*

consegnati e le altre informazioni non più necessarie per il funzionamento e la fornitura dei Servizi saranno eliminati dai nostri server. Si tenga presente che, eliminando i nostri Servizi dal dispositivo senza usare l'apposita funzione presente nell'applicazione, le informazioni potrebbero rimanere archiviate per un periodo più lungo. L'utente deve inoltre essere consapevole del fatto che, quando elimina l'account, le informazioni in possesso degli altri utenti non subiranno modifiche, così come la copia dei messaggi inviati in loro possesso.

Legge e protezione - *WhatsApp può accedere alle informazioni nonché raccoglierle, utilizzarle e condividerle qualora ritenesse in buona fede che ciò sia necessario per: (a) rispondere, ai sensi della legge o dei regolamenti applicabili, ai procedimenti legali o alle richieste governative; (b) applicare i nostri Termini e altre condizioni e informative applicabili, anche a scopo di analisi di potenziali violazioni; (c) individuare, analizzare, prevenire e gestire frodi e altre attività illegali o problemi tecnici o di sicurezza; (d) proteggere i diritti, la proprietà e la sicurezza dei nostri utenti, di WhatsApp, del gruppo di aziende di Facebook o di terzi.*

Operazioni a livello globale - *L'utente accetta le nostre procedure relative alle informazioni, ivi incluse la raccolta, l'utilizzo, l'elaborazione e la condivisione delle informazioni in base alla descrizione contenuta nella presente Informativa sulla privacy nonché il trasferimento e l'elaborazione delle informazioni negli Stati Uniti e in altre nazioni a livello globale in cui sono presenti le nostre strutture, i nostri fornitori di servizi o i nostri partner, indipendentemente dal luogo in cui vengano utilizzati i nostri Servizi. L'utente riconosce che le leggi, le norme e gli standard della nazione in cui vengono archiviate o elaborate le sue informazioni personali potrebbero essere diversi da quelli vigenti nella sua nazione.*

Aggiornamenti all'informativa - *WhatsApp si riserva il diritto di modificare o aggiornare l'Informativa sulla privacy. Comunicheremo le modifiche all'Informativa sulla privacy nel modo ritenuto più opportuno e aggiorneremo la data di "Ultima modifica" nella parte superiore della presente Informativa. L'ininterrotto uso dei Servizi comporterà l'accettazione dell'Informativa sulla privacy così modificata. Se non accetta l'Informativa sulla privacy così modificata, l'utente deve interrompere l'utilizzo dei Servizi. Consigliamo la consultazione periodica dell'Informativa sulla privacy.*

Assistenza - *Per qualsiasi domanda sull'Informativa sulla privacy, è possibile contattarci.*
WhatsApp Inc. Privacy Policy 1601 Willow Road Menlo Park, California 94025 Stati Uniti d'America

3.2. LE *PRIVACY POLICIES* DI TIPO "*USER-CENTRIC*" E "*DATA-CENTRIC*". *STICKY PRIVACY POLICIES.*

Le politiche di *privacy user centric* consentono all'utente di personalizzare le proprie *preferences* mantenendo il controllo in termini di accesso, visibilità e utilizzo. Il controllo può essere più o meno esteso a seconda che il set di opzioni è comunque definito dal provider del servizio oppure dallo stesso utente.

Il primo caso è quello tipico dei social media, in cui l'utente sulla base di regole predefinite può modificare i *default settings* del servizio, tuttavia rimanendo nel dominio delle opzioni definite dal provider che al più possono essere combinate.

Il secondo caso comprende politiche *user-centric vere e proprie - User Privacy Policies - UPP*, che consentono all'utente non solo la scelta delle opzioni ma anche di definire e dichiarare le proprie regole, in forma affine a quella contrattuale, e tenendo conto del dominio di utenza, delle tipologie di dato e degli attributi da questo esposte.

L'utente può definire ogni elemento della politica: il dato da tracciare comprensivo dei suoi attributi; il proprietario, il destinatario, le specifiche di accesso e di restrizione parziale o totale.

Le principali criticità nella definizione delle politiche *user-centric* attengono: i) l'attuazione e il mantenimento dell'*usabilità; ii)* l'eccessiva lunghezza della descrizione e l'ambiguità del contenuto; *iii)* la scarsa visibilità in termini di informativa degli aggiornamenti e della comunicazione sulle conseguenze e sull'impatto pratico di una determinata regola di *privacy; iv)* la scarsa informativa e consapevolezza nell'utente dell'importanza della *privacy* quindi la conseguente incapacità di calibrare l'impostazione in coerenza alle proprie aspettative e necessità; *v)* la diversa percezione del significato, delle aspettative e della necessità di *privacy* associabile ai diversi contesti culturali e tecnologici.

Ciò premesso un efficace disegno di politiche *user-centric* dovrebbe prevedere: *i)* un aumento dell'usabilità: l'utente dovrebbe trovare l'adeguata configurazione di privacy con pochi e chiari passaggi; disporre o definire non troppe opzioni ma quelle giuste; *ii)* in analogia al precedente punto anche la lunghezza delle regole dovrebbe trovare un compromesso tra l'essere complete ma non ridondanti e tali da scoraggiarne la lettura e l'applicazione, e l'essere essenziali ma non incomplete; *iii)* esporre anteprime degli effetti e dell'impatto di una regola e della sua impostazione; *iv)* mantenere informati gli utenti sugli aggiornamento delle regole di *privacy*.

STICKY PRIVACY POLICIES.

Le *Sticky Policies* sono insieme di regole associate e "*impacchettate*" ai relativi dati, nascono come strumenti di *Privacy Enhancing Technologies* (*PETs*) per la trasmissione sicura di informazioni confidenziali tra una rete di utenti limitata e comunque chiusa, in cui la cifratura delle informazioni si rivela una soluzione tecnica ottimale per proteggere lo scambio *end-to-end* di dati. In tal senso gli standard di cifratura e di firma digitale *Public-Key Cryptography Standards* (*PKCS#7)* e *Secure/Multipurpose Internet Mail Extensions* (*S/MIME)* o le specificazioni *World Wide Web Consortium* (*W3C*) *XML Encryption* e *XML Signature* possono considerarsi embrionali esempi di *Sticky Policies* in cui le regole attengono prescrizioni applicative tecniche necessarie per l'utilizzo degli algoritmi di cifratura e delle modalità di codifica/decodifica del messaggio.

L'elemento informativo al quale le *Sticky Policies* si associano e si applicano può comprendere: *i)* contenuti (es. dati e profili personali, messaggi, documenti, media); ma anche *ii)* ulteriori regole (azioni o obbligazioni) derivanti da vincoli decisionali dinamici al variare dei possibili contesti applicativi in cui le *Sticky Policies* sono processate.

Ad esempio è questo il caso in cui ad una richiesta di rilascio (accesso e/o utilizzo) di un record di *PII Personal Identifying Information)* segue una decisione positiva (*grant*) la cui *esecuzione* è però condizionata da regole aggiuntive - prescritte da opportune *Sticky Privacy Policies,* che fissano delle eccezioni negandone (*deny*) o limitandone il rilascio verso particolari servizi in ragione (per esempio) di un aggiornamento che il soggetto interessato ha prodotto sulla propria lista di siti indesiderati (*black list*).

Oppure il caso in cui ad una richiesta di accesso ad un documento confidenziale (es. record sanitario) segue una decisione positiva (*grant*) la cui *esecuzione* è però condizionata da una ulteriore regola che ne prescrive la cancellazione dopo un certo intervallo di tempo.

Le *Sticky Policies* si basano sull'utilizzo di metadati esplicativi per associare dati, risorse e azioni alle condizioni di accesso e utilizzo; tale associazione può essere implementata con una una logica di tipo *fine-grained* (a grana fine) rispetto al numero degli attributi e dei vincoli introdotti dall'utente o dal soggetto decisore (*Policy Owner, Policy Iusser*). La risultante entità di contenuti e regole di controllo deve essere considerata e processata come un unico blocco di informazione (*Data Package).*

```
<data package>
  <data component>  // Identity and profile - attribute 1
      <sticky policy> // disclosure policy – IBE encryption key
         <Trusted Authority>
            address and location of the Trusted Authority
         </Trusted Authority>
         <owner>
         //reference name – IBE  encryption key
            <reference name> pseudonym1 </reference name>
            //encrypted call back address
             //by using the user's reference name
            <owner's details>
            encrypted call back address
            <owner's details>
         </owner>
         <target>
            name of the identity or profile attribute
         </target>
         <validity>
            expiration date
         </validity>
          <constraint>
            require_strong_X.509_authentication
         </constraint>
         <constraint>
            allow_sharing_of_data
         </constraint>
            <action>
            notify_owner
            </action>
      </sticky policy>
      <encrypted data>
         encrypted attribute value,
         using the above policy as IBE public key
       </encrypted data>
   </data component>
</data package>
```

Figura 3.3. - *Esempio di Sticky Privacy Policies*[233]

Un elenco delle possibili tipologie di *Sticky Policy* è prodotto da *Chadwick* e *Fatema*[234]. Ogni politica è distinta da un autore e dal particolare linguaggio utilizzato.

1. *Authorization Policies*: prescrivono azioni e attori sulle risorse "*agganciate*" alle *Sticky Policy;*
2. *Conflic R:esolution Policy:* prescrive come risolvere i conflitti sulle decisioni di accesso e utilizzo delle risorse;
3. *Audit Policies:* prescrive quali informazioni accessorie controllare in fase di analisi e esecuzione della politica;
4. *Obligation Policies:* è correlata alla precedente e prescrive quali azioni eseguire;
5. *Privacy Policies:* prescrive tipiche informazioni di controllo sulle informazioni personali

[233] Cfr MONT CASASSA M., PEARSON S., BRAMHALL, P., *Towards accountable management of identity and privacy: sticky policies and enforceable tracing services, Database and Expert Systems Applications, 2003,* Proceedings. 14th International Workshop on Year: 2003, p. 377 – 382 (2003)

[234] Chadwick David W., Fatema Kaniz, *An advanced policy based authorisation infrastructure,* DIM '09: Proceedings of the 5th ACM workshop on Digital Identity Management (2009)

quali ad esempio il periodo di utilizzo, la finalità le eccezioni;

6. *Authentication Policy:* è agganciata alla precedente e alla prima (Authorization Policy) e prescrive il livello di affidabilità di chi è autorizzato all'utilizzo delle risorse informative e d in particolari delle informazioni personali;
7. *Data Manipulation Policy*: prescrive dettagli di trattamento delle le risorse vincolate alle prescrizione delle *Sticky Policies*: come tali risorse, in particolare informazioni personali possono essere *modificate, integrate o aggregate ad altre informazioni appartenenti allo stesso soggeto o ad altri soggetti*

3.3. I FRAMEWORK E I LINGUAGGI.

Le politiche e le impostazioni di *privacy* sono definite e gestite tramite linguaggi e framework associati, che nel loro insieme configurano un sistema di *Policy Based Access Control (PBAC)* composto dai seguenti componenti implementanti le funzioni di analisi *(parsing),* processamento (*process)* ed esecuzione *(enforcement)* delle politiche[235].

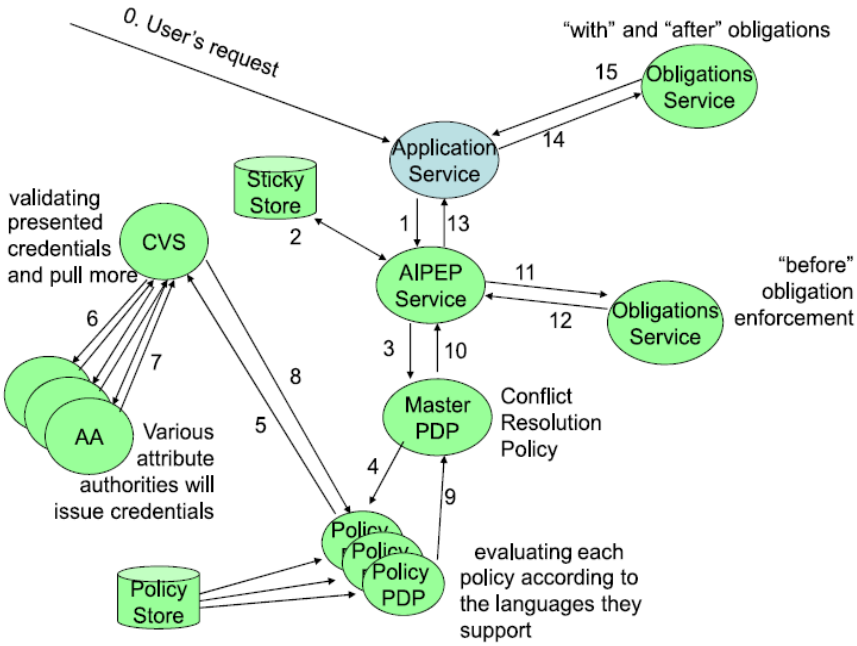


Figura 3.4. - Componenti di un sistema *Policy Based Access Control (PBAC)*[236]

1. *Policy Administration Point (PAP)*: crea le politiche archiviate nel *Policy Store* o nello *Sticky Store;*
2. *Policy Decision Point (PDP)*: combina le politiche per produrre la decisione risultante;
3. *Policy Enforcement Point (PEP)*: analizza le richieste di accesso e utilizzo delle risorse; nonché la politica per sottoporla alla decisione del *PDP*; a decisione prodotta, esegue e applica la politica;
4. *Policy Information Point (PIP):* fornisce attributi di supporto alla decisione del *PDP;*

[235] Cfr CHADWICK DAVID W., FATEMA KANIZ, *An advanced policy based authorisation infrastructure,* DIM '09: Proceedings of the 5th ACM workshop on Digital Identity Management (2009)

[236] Cfr CHADWICK D.W., LIEVENS S.F., HARTOG DEN J. I., PASHALIDIS A., ALHADEFF J., *My Private Cloud Overview: A Trust, Privacy and Security Infrastructure for the Cloud, Cloud Computing (CLOUD),* 2011 IEEE International Conference on Year: 2011, p. 752 – 753

queste informazioni aggiuntive possono essere attinenti al titolare *(Data Subject)* della politica o a chi la rilascia *(Data Iusser);* alla risorsa oggetto della richiesta di accesso e utilizzo o al contesto in cui questa viene processata. Il *Policy Information Point,* quindi, a sua volta comprende il *Credential Validation Service (CVS)* e l'*AA (Attribute Authorities)* per la convalida delle credenziali;

5. *Obligation Service (OS):* implementa azioni di notifica o di logging;
6. *Conflict resolution Service (CRS):* risolve possibili collisioni sulle decisioni.

I principali linguaggi di implementativi di un sistema *PBAC* si distinguono per funzionalità, insieme di regole implementate e per proprietà.

Short	Property	Comment
ME	Machine-Enforceable	The policies are enforceable by a policy engine.
CO	Constraints and Obligations	Express constraints and obligations on set policies.
PU	Purpose	Express the purpose of a policy in an informal way. The policy can only be used for this purpose.
EX	Extensibility	Easily extendible at runtime without interruptions.
RD	Rights and Dispensations	Express the granting of rights to perform certain actions and the dispensation of those rights.
CR	Conflict Resolution	The identification and resolution of contradictory statements.
SA	Speech Acts	Actions such as delegation and revocation of rights, request for a right and the cancellation of that request.
RE	Reasoning	Possibility to (automatically) reason with given policies or expressions in a language.
IF	Information Flow Control	Possibility to control where information goes after posting it.
ER	Expressive Rules	Rules that make it possible to express any possible privacy, e.g. negative authorisation, completeness.
UR	Unambiguous Representation	Representing expressions in a way that is unambiguous for both the privacy user and the framework.
SP	Scalable and Performant	Scales well and has an acceptable speed performance.
DI	Distributivity	Distributive design, lessening the workload of the server and protecting from system failure.
IP	Indexing of Policies	Possibility to assign an index to a policy for easy lookup.

Figura 3.5. - Proprietà di un sistema *Policy Based Access Control (PBAC)*[237]

I principali linguaggi sono: *RBAC - Role-Based Access Control, P3P - Platform for Privacy Preferences, EPAL - Enterprise Privacy Authorization Language, LPU - Logic of Privacy and Utility,*

[237] Cfr NICOLAS VANDEN BOSSCHE, *Adaptive Privacy Modelling for Social Networking Sites,* Dissertation handed in to achieve the academic title of Master in civil engineering, computer science A.A. 2011-2012 p. 8

XACML - eXtensible Access Control Markup Language, Rei, Ponder and Ponder2, KAoS il cui incrocio con le precedenti proprietà è rappresentato nella seguente figura.

	RBAC	P3P	EPAL	LPU	XACML	Rei	Ponder	Ponder 2	KAoS
ME	●		●		●		●	●	●
CO		●	●	●	●	●	●	●	●
PU		●	●						
EX					○	●			●
RD	●	○	○	●		●	●	●	
CR				○	●	●			
SA	○			○		●	●	●	●
RE					○	●			●
IF				●					
ER			●	●	○	●			●
UR	●	○	●	●	●	●	○	○	●
SP					●			●	
DI	○				●			●	
IP			○		○				

Figura 3.6. - Incrocio Proprietà/Framework di un sistema *Policy Based Access Control (PBAC)*[238]

[238] Cfr NICOLAS VANDEN BOSSCHE, *Adaptive Privacy Modelling for Social Networking Sites,* Dissertation handed in to achieve the academic title of Master in civil engineering, computer science A.A. 2011-2012 p. 13

4. QUESTIONI APERTE.

Se l'obiettivo è aumentare la *privacy* e potenziare la protezione dei dati personali, tutte le misure che possano o meno essere rigorosamente categorizzate in misure di sicurezza, di controllo degli accessi o specificatamente di *privacy* possono essere considerate aumentanti la protezione sui dati personali e quindi considerabili *PETs, Privacy Enhancing Technologies*. Si rivela tale la cifratura se strumentale alla pseudonimizzazione, oppure una sticky policies se concorre ad evitare il *disclosure* di un dato personale ad un utente non autorizzato con lo stesso effetto che si otterrebbe cifrando il dato, rendendolo incomprensibile e quindi inaccessibile ad un determinato utente o a gruppi di utenti.

Le PETs costituiscono effettivamente contromisure operative per la privacy?

Alle più diffuse tipologie di transazioni on-line ne corrispondono di equivalenti più protettive per la *privacy:*

a) al browsing in chiaro corrisponde TOR (The Onion Router): un sistema di comunicazione anonima per Internet basato sulla seconda generazione del protocollo di rete di onion routing. L'utilizzo di TOR rende è molto più difficile tracciare l'attività Internet dell'utente, TOR consente di proteggere la privacy degli utenti, la loro libertà e la possibilità di condurre delle comunicazioni confidenziali senza che vengano monitorate;

b) per gli acquisti con carta di credito la controparte PETs può essere rappresentata dai bitcoins: la rete Bitcoin consente il possesso e il trasferimento anonimo delle monete; i dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più personal computer sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca.

c) per le comunicazioni via email la versione PETs è rappresentata dalle applicazioni S/MIME e PGP che consentono a chiunque disponga di una coppia di chiavi asimmetriche certificate di scambiare messaggi in totale riservatezza, garanzia di integrità e autenticità.

La risposta è quindi affermativa. Ma non possono non rilevarsi delle limitazioni in ragione allo scarso utilizzo e alla scarsa diffusione di queste contromisure.

Parte delle limitazioni è riconducibile allo scarso successo di mercato: la maggior parte delle contromisure di *privacy* non vengono utilizzate e le decisioni degli utenti in ordine alla protezione delle proprie informazioni personali sembrano andare nella direzione opposta perché il mercato favorisce e tende a far prevalere sistemi di applicazioni che *di per se, by default*

non proteggono la privacy.

La limitazione quindi non risiede nell'influenza esercitata dal mercato quale attore di *reveal preferences,* bensì nel fatto che le PETs non sono tecnologie *by design/default* nelle applicazioni di browsing, di posta elettronica, di pagamenti anonimi.

Il successo delle contromisure di *privacy* non è più misurabile nell'essere configurabili come applicazioni o nell'utilizzare algoritmi robusti, bensì nell'essere o meno le tecnologie di default, atteso che l'utente (il consumatore) segue e consolida il punto di partenza, lo *status quo,* tendendo a far propri e mantenere i *default settings*.

5. LA PROTEZIONE DEI DATI PERSONALI COME REQUISITO INTRINSECO DI PROCESSI E SERVIZI.

5.1 IL FRAMEWORK *PRIVACY BY DESIGN E PRIVACY BY DEFAULT.*

Il concetto di *privacy by design* risale al 2010, già presente negli Usa e Canada e poi adottato nel corso della 32ma Conferenza mondiale dei Garanti privacy. La definizione fu coniata da Ann Cavoukian, Privacy Commissioner dell'Ontario (Canada). Esso si basa sui seguenti principi fondamentali[239]:

1. *Proactive not Reactive; Preventative not Remedial* - prevenire non correggere, i problemi vanno valutati nella fase di progettazione: *l'approccio Privacy by Design è caratterizzato da misure proattive piuttosto che reattive. Anticipa e previene gli eventi invasivi della privacy prima che accadano. Non onsegue ai rischi per la privacy per porre in essere l'intervento, né offre rimedi per risolvere le violazioni della privacy una volta che si sono verificate, mirando piuttosto ad impedirne l'accadimento. Privacy by Design viene prima non dopo.*

2. *Privacy as the Default - privacy* come impostazione di default: *Privacy by Design punta a fornire il massimo grado di privacy garantendo che i dati personali siano automaticamente protetti in qualsiasi sistema informatico o pratica commerciale. Se un individuo non fa nulla, la privacy rimane inalterata, quindi nessuna azione è necessaria o richiesta all'individuo per proteggerla.*

3. *Privacy Embedded into Design* - privacy incorporata nel progetto: *Privacy by Design è integrato nella progettazione e nell'architettura dei sistemi informatici e delle pratiche commerciali. Non è un elemento incastrato come un add-on, a violazione avvenuta. Il risultato è che la privacy diventa una componente essenziale del sistema, parte integrante senza invaderne o limitarne le funzionalità.*

4. *Full Functionality – Positive-Sum, not Zero-Sum* - massima funzionalità, in maniera da rispettare tutte le esigenze: *Privacy by Design punta a incrociare tutti gli interessi e gli obiettivi legittimi non attraverso un approccio orientato al compromesso. Evita la pretesa di false dicotomie, come la privacy contro la sicurezza, dimostrando che è possibile, e molto più auspicabile, disporre di entrambi.*

5. *End-to-End Security – Lifecycle Protection* - sicurezza durante tutto il ciclo del prodotto o

[239] CFR CAVOUKIAN ANN, *Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (2013)

servizio: *Privacy by Design, essendo stato incorporato nativamente nel sistema si estende in modo sicuro per tutto il ciclo di vita dei dati coinvolti. Deve contare su misure di sicurezza forti, e assicura che tutti i dati siano conservati in modo sicuro, quindi distrutti a fine processo quando non più necessari.*

6. *Visibility and Transparency* – trasparenza: *Privacy by Design cerca di assicurare a tutti i soggetti interessati qualunque sia la pratica commerciale o la tecnologia, ed in coerenza agli obiettivi dichiarati. Componenti e procedure rimangono visibili, trasparenti e soprattutto verificabili.*

7. *Respect for User Privacy* - centralità dell'utente: *Privacy by Design richiede a tutti gli stakeholders coinvolti di mantenere centrali gli interessi dell'individuo, esponendo default settings forti, informativa accurata esposta con modalità user-friendly.*

CAPITOLO 4

VERSO LA PRIVACY 2.0:
NUOVI SCENARI DI RISCHIO E NUOVE SEMANTICHE

SOMMARIO: 1. Gli scenari ed alcuni esempi di rischio in contesti di forte inferenza informativa. – **1.1.** *"Internet of Things"*. – **1.2.** *Apps* per *smart-devices*. – **1.3.** *"Big Data"* e *Data Mining*. – **1.4.** Realtà aumentata e *Data Accretion*. – **2.** Le nuove forme di vulnerabilità e di rischio per la protezione dei dati personali. – **2.1.** Asimmetria Informativa. Dispersione del controllo sui dati personali. Perdita di qualità del consenso. – **2.2.** Difetto di trasparenza. Eccesso di dati personali. Molteplicità delle finalità. – **2.3.** Eccesso di esposizione dell'utente. Deduzione invasiva di profili. – **2.4.** Difetto di *Privacy by Design/Default*. Pluralità dei titolari di trattamento. – **3.** La garanzia di qualità dei dati e le nuove tipologie di rischio per la *Privacy*. – **4.** Le nuove proprietà del Dato Personale. – **4.1.** Proprietà e possesso del Dato Personale. *Personal Data Store*. **4.2.** I dati personali a soggetti multipli. *Multiple Subjects Personal Data*. – **4.3.** Il valore economico dei Dati Personali e della *Privacy*.

1. GLI SCENARI ED ALCUNI ESEMPI DI RISCHIO IN CONTESTI DI FORTE INFERENZA INFORMATIVA.

Nella prima parte di questo capitolo verranno illustrati quattro scenari informazionali distinti da una massiva produzione e un pervasivo scambio di dati; dati che possono essere creati e rilasciati volontariamente dagli utenti (soggetti interessati o altri attori), prodotti involontariamente da *non-utenti,* oppure generati da *cose;* acceduti o archiviati su dispositivi. Questi volumi di dati potranno quindi essere raccolti e trasferiti in piattaforme *Cloud,* (ri)allocati e (ri)utilizzati; processati - attraverso algoritmi di analisi predittive incrociate (quantitative e qualitative) e da sistemi applicativi di *find engine*[240], per produrre inferenza e ulteriore informazione volta ad collegare dati e relazionare fenomeni; *aumentare* e *migliorare* la realtà. Tutto ciò espone agli utenti una personalizzazione che può essere foriera di vantaggi: servizi a valore aggiunto (più efficienti e meno costosi) migliorativi della *user-experience* in svariati e molteplici possibili ambiti[241]; ma anche di possibili svantaggi: esposizioni

[240] Nella parte dell'elaborato che segue, l'espressione *find engine* indicherà l'insieme di applicazioni collocate generalmente in *cloud* che in risposta a specifiche richieste degli utenti, aggregano processano grandi volumi di dati per analizzarne gli attributi descrittivi (qualitativi e quantitativi) mediante algoritmi di definizione ed estrazione di attributi (tra gli altri: *data mining, machine learning, hashing, crowdsourcing*), al fine di estrarre collegamenti, effettuare analisi predittive, relazionare specifici fenomeni.
Un tipica applicazione di *find engine* è il motore di ricerca.

[241] In argomento per i possibili esempi si rimanda al capitolo 2 -.*Privacy e Protezione dei Dati personali: pluralità semantiche e criticità.,* paragrafo 1. - *I dati e le informazioni personali.*

informazionali inattese, indesiderate, fastidiose, non autorizzate o al limite pericolose.

I contesti disaminati sono: *Internet of Things, App* per *smart-devices, "Big Data"* e *Data Mining,* Realtà Aumentata e *Data Accretion.* Ognuno di essi viene preliminarmente descritto nelle sue caratteristiche tecniche e con l'ausilio di alcuni esempi viene evidenziato come e in quale misura i dati personali incidono sulla loro configurazione e sul loro funzionamento. Viceversa, in ragione del fatto che ognuno di questi scenari implica il trattamento di dati personali, saranno attenzionati i seguenti elementi comuni: *i)* l'individuazione della base giuridica; *ii)* la connotazione al ruolo di titolare e di responsabile degli attori coinvolti, oltre al soggetto interessato (c.d filiera dei portatori di interessi); *iii)* le nuove forme di vulnerabilità e di rischio, presupposti di successive violazioni per i dati personali.

Quanto al primo punto, il diritto applicabile è rappresentato da due atti regolatori: il nuovo regolamento europeo per la protezione dei dati personali 679/2016, in particolare nelle parti in cui regola: la definizione di dato personale[242]; l'ambito territoriale del trattamento[243]; i principi di protezione dei dati personali (qualità, minimizzazione e finalità)[244]; i requisiti di legittimità del trattamento (in cui sussistano e siano rispettate le condizioni di consenso, finalizzazione di obblighi contrattuali, il legittimo interesse, l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri)[245]; la garanzia per il soggetto interessato di esercitare i propri diritti (trasparenza, accesso, rettifica, cancellazione, opposizione al trattamento, portabilità)[246,247].

In aggiunta al GDPR si colloca la Direttiva *e-privacy* 2002/58/CE[248] modificata dalla Direttiva 2009/136/CE. In particolare, per l'attinenza regolatoria dei trattamenti posti in essere in ambito *IoT* e *Apps,* occorre richiamarne il considerando 24) che recita:

> *<Le apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali>*

---

242 Cfr GDPR Art. 4 *Definizioni,* comma 1);

243 Cfr GDPR Art. 3 *Ambito di applicazione territoriale;*

244 Cfr GDPR Art. 5 *Principi applicabili al trattamento di dati personali;*

245 Cfr GDPR Art. 6 *Liceità del trattamento;* Art. 7 *Condizioni per il consenso*

246 Cfr GDPR Capo III *Diritti dell'Interessato* art. 12, 13, 14 - *Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato;* art. 15 *Diritto di accesso dell'interessato;* art. 16 *Diritto di rettifica;* art. 17 *Diritto alla cancellazione («diritto all'oblio»);* art. 18 *Diritto di limitazione di trattamento;* art. 20 *Diritto alla portabilità dei dati;* art. 21, 22 *Diritto di opposizione.*

247 Per il dettaglio degli elementi elencati si rimanda al capitolo 1 – *Lo scenario normativo attuale. Questioni aperte;* Paragrafi 3 - *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: le principali novità.* Paragrafo 4 - *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: il soggetto interessato e il dato personale.*

248 Direttiva 2002/58/CE del Parlamento Europeo e del Consiglio, 12 Luglio 2002, r*elativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche)* - L 201/37 pubblicato nella GUUE del 31.07.2002 e successive modifiche.

e l'art. 5, paragrafo 3) che – con riferimento a tutte le informazioni anche non personali, recita:

> *<l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva 95/46/CE, tra l'altro sugli scopi del trattamento*>, <...>.

Quanto al secondo punto ogni attore componente la filiera dei portatori di interesse[249] può essere considerato titolare o responsabile del trattamento dei dati personali nella misura in cui autonomamente definisce gestisce le regole e gli algoritmi di processamento delle informazioni, i mezzi e le finalità di trattamento per scambiare, interconnettere, (ri)allocare e (ri)utilizzare i dati trattati (iniziali e ricavati) in relazione agli usi e agli scopi (principali e secondari).

Il GDPR impone ai (con)titolari del trattamento (e ai responsabili) di adottare le misure tecniche e organizzative per garantire e comprovare la conformità al regolamento e l'efficace attuazione dei principi di protezione dei dati rispetto ai quali si distinguono gli obblighi di trasparenza, liceità e mantenimento dei requisiti di qualità; ciò secondo un approccio pro-attivo di tipo *by design / default* che tenga conto – in fase di progettazione del trattamento stesso, della sua natura, dell'ambito di applicazione, del contesto, delle finalità, dei rischi e dell'impatto del trattamento sui diritti e le libertà delle persone[250]. Le decisioni assunte dal titolare e dal responsabile devono essere proporzionate tanto al rischio (prima) tanto al danno (dopo).

Il principio di *accountability* che il GDPR pone in capo al titolare e al responsabile, attiene non solo l'autodeterminazione delle politiche del trattamento ma anche la gestione delle conseguenze dello stesso in caso di violazioni sui dati personali; impone ad entrambi oltre a una valutazione *ex ante* di impatto e di rischio anche una valutazione prudenziale *ex post* - a violazione avvenuta, volta ad analizzarne la gravità, quindi eventualmente ad attuare gli obblighi di comunicazione e di notifica diversificandone l'attore destinatario: verso l'Autorità Garante Nazionale o Europea (in caso di trattamenti transnazionali) oppure verso il soggetto interessato nel caso in cui la gravità della violazione sia tale da generare conseguenze misurabili e dirette sui diritti e le libertà della persona.

---

[249] La filiera dei portatori di interesse comprende almeno: i fabbricanti di dispositivi, gli sviluppatori di sistemi operativi e di applicazioni, i gestori di piattaforme di dati o degli *app store,* i noleggiatori/noleggianti di dispositivi; terze parti quali, ad esempio, gestori di piattaforme sociali o *applicazioni cloud* per l'hosting e l'analisi dei dati raccolti; organismi regolatori di normazione.

[250] Cfr GDPR Art. 24 *Responsabilità del titolare del trattamento;* Art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita;* Art. 28 *Responsabile del trattamento; Art. 32 Sicurezza del trattamento;* Art. 35 *Valutazione d'impatto sulla protezione dei dati;* Art. 37, 38, 39 *Designazione, posizione e compiti del responsabile per la protezione dei dati personali.*

Il terzo punto riveste la parte più importante del capitolo oltre ad essere centrale per l'elaborato stesso; in dettaglio è trattata al paragrafo 2 - L*e nuove forme di vulnerabilità e di rischio per la protezione dei dati personali.* Essa trae origine ed è stata sviluppata sulla seguente considerazione: i quattro contesti informazionali di seguito disaminati concorrono di fatto – seppur con forme e approcci implementativi diversi, ad avviare e mantenere il c.d. *schema di trattamento Big Data;* esso si basa sulla produzione massiva di volumi di dati e dal successivo arricchimento qualitativo e quantitativo per il tramite di attributi descrittivi che, analizzati, ne aumentano la sfera di significato, di influenza e di sovrapponibilità semantica con quella di altri dati. L'attore che determina le relazione tra i dati sulla base della loro quantità, tipologia, rilevanza e pertinenza è un artefatto algoritmico[251], il cui utilizzo e gestione sono prerogativa del titolare del trattamento. *Algoritmo e titolare* rappresentano, quindi, un sistema che media tra i dati e l'utente; tra il valore e le caratteristiche delle informazioni e l'utilizzo che ne richiede il soggetto interessato in termini servizi, applicazioni e comunicazione.

Le criticità sorgono quando questa mediazione non è asettica, quando non si mantiene trasparente e neutrale disattendendo le aspettative e le richieste dei soggetti interessati; quando – senza che il soggetto interessato sia stato informato, sia consapevole o abbia nello specifico acconsentito, le sfere di pertinenza dei dati (in quanto tali) si sovrappongono, collidono o peggio sostituiscono l'ambito privato, le cose appartenenti alla persona o le informazioni rilasciate da questa in altri contesti .

Le vulnerabilità si delineano quando il risultato dell'*algoritmo (find engine)* interseca descrittori per trovare nuove relazioni e quindi nuovi dati attinenti l'identità, le abitudini, gli amici, gli interessi, i luoghi di una persona; la sua salute o la sua sicurezza senza che questo rientri nelle aspettative degli utenti, prevalga sulla loro autodeterminazione o sia loro omesso.

I rischi si configurano nel momento stesso in cui degenera il carico informativo tra il *find engine* (l'algoritmo) e la persona, il consenso rilasciato da quest'ultima perde di efficacia, il trattamento che ne consegue diventa sconosciuto, indesiderato, fastidioso, discriminatorio comunque dannoso per il soggetto interessato; il dato personale totalmente fuori controllo.

La violazione trova attuazione quando si passa da un pericolo eventuale ad un pericolo certo o avvenuto che si misura nell'accadimento del furto, della perdita, della modifica o comunque dell'utilizzo illecito delle informazioni personali: oramai il danno è fatto, vulnerabilità e rischio permangono a monte.

[251] Questa espressione racchiude l'insieme delle tecniche, delle metodologie e delle regole statistiche, nonché le applicazioni che su queste si basano per analizzare le caratteristiche quantitative e qualitative dei dati, processare gli attributi descrittivi al fine di estrarne di nuovi in esito a specifiche richieste. Si citano ad esempio le applicazioni di *find engine;* gli algoritmi di d*ata mining,* di *machine learning,* di *crowdsourcing,* di *hashing,* di classificazione semantica.

1.1. "*INTERNET OF THINGS*".

Internet of Things[252] (*IoT,* Internet degli Oggetti) indica un insieme di tecnologie (principalmente basate su radio frequenza, wireless, reti elettriche di tipo *low power* o *power line*)[253] che permettono di collegare a Internet qualunque tipo di oggetto - anche di per se "*off-line, spento",* modificandone le funzioni, dotandolo di "*intelligenza*" o più semplicemente di *interconnettività* ovvero della capacità di attivarsi e disattivarsi autonomamente, raccogliere e trasferire dati che potranno essere successivamente riutilizzati in svariati possibili contesti: energia, telecomunicazioni, domotica, salute, sport, mobilità, etc.

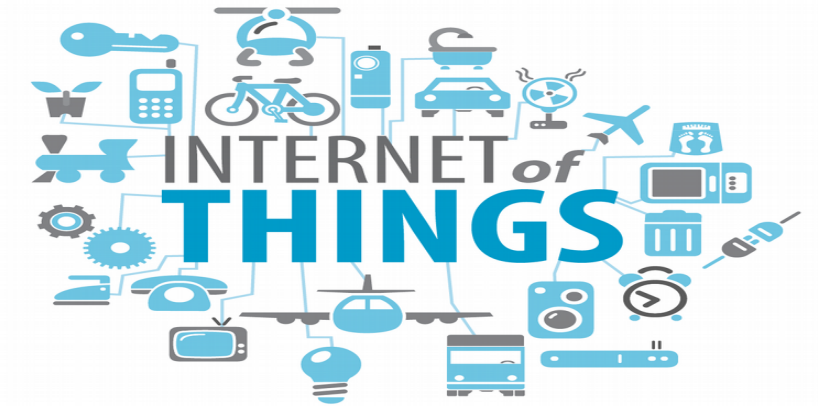


Figura 4.1 – *Devices sensorizzati* componenti l'*Internet of Things*[254]
L'*IoT* - secondo un modello descrittivo ISO[255], consta nell'interconnessione tramite Internet di svariati oggetti e dispositivi in modo da moltiplicare le modalità di interazione e inter-processamento finalizzate alla creazione di nuovi servizi e modelli di business.

Tra i numerosi progetti *IoT*, ed al fine di rappresentare la concomitanza tra vantaggi e criticità, si cita (richiamandolo nel proseguo del paragrafo) il progetto *Energy@Home*[256] - al quale partecipa un cartello di operatori del settore telefonia-domotica-energia (es. Tim, Vodafone; Whirpool, Indesit; Enel).

Tale progetto e la relativa infrastruttura hanno come obiettivo la raccolta di dati relativi alle persone nel loro ambiente domestico, veicolati ed interconnessi da un comune protocollo, con la principale finalità di bilanciare ed ottimizzare i consumi e quindi, sostanzialmente, beneficiare l'utente (partecipante al progetto) con un risparmio in bolletta.

---

[252] *IoT* è un neologismo introdotto nel 1999 per la prima volta da Kevin Ashton (ricercatore presso il MIT, Massachussets Institute of Technology), collegato all'esigenza di dare un nome agli oggetti reali connessi ad Internet.

[253] Per un ulteriore approfondimento sull'argomento, si indica: *IoT* Library - *Le 8 tecnologie alla base dell'Internet of Things: RFid, Personal Area Network, Wi-Fi. Ma anche reti Mesh e cellulari. Ecco le principali tecnologie disponibili in ambito IoT,* raggruppate in otto cluster dall'Osservatorio *Internet of Things* del Politecnico di Milano; Vincenzo Zaglio, 18 giugno 2013 – disponibile alla risorsa: http://www.internet4things.it/iot-library/le-8-tecnologie-alla-base-dell-internet-of-things/

[254] Fonte Business.it, disponibile alla risorsa: http://www.business.it/internet-of-things-tutti-i-numeri-del-business/

[255] https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf

[256] Cfr http://www.energy-home.it/SitePages/Home.aspx

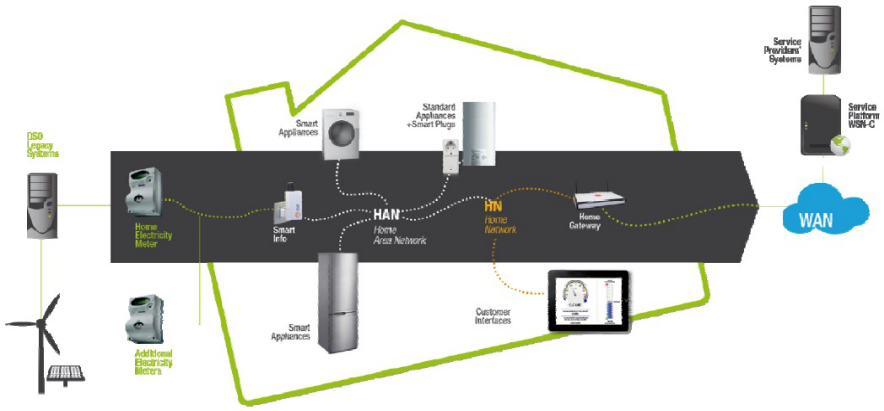


Figura 4.2 - Architettura *IoT* del progetto Energy@Home[257]

Tornando alle caratteristiche, *IoT* indica una infrastruttura risultante di milioni e milioni di sensori[258] - di per se dotati di limitata capacità elaborativa, nativamente interconnessi e che soddisfano almeno le seguenti caratteristiche principali[259]:

i. risultare a se stanti (es. tag *RFId, Radio-Frequency Identification*) oppure integrati in svariati e diversi oggetti: di uso quotidiano (es. occhiali, orologi, scarpe), dispositivi *intelligenti* (es. *smartphone*, *tablet, laptop);* in oggetti di utilizzo domestico (es. lampadine, termostati o elettrodomestici); oppure in rilevatori di luminosità, movimento, temperatura, umidità; rilevatori ambientali o territoriali; videocamere, microfoni; od ancora in misuratori di *performance;*

ii. essere dotati di identificativi univoci e, quindi, interconnessi gli uni con gli altri, con altri oggetti o dispositivi; ma, in particolare interconnessi con sistemi (anche distribuiti) di processamento *back-end;* piattaforme di *hosting* e analisi dei dati (in *Cloud;* oppure affini a *Google Universal Analytics*); non ultimi a sistemi di *Data Mining;*

iii. essere interfacciabili con applicazioni terze - per il tramite di *API* (*Application Programming Interface)* in genere definite ed esposte dal fabbricante del dispositivo, che consentono agli sviluppatori di applicazioni di accedere alle funzionalità base generali, quali ad esempio la tipologia di dati e la frequenza di raccolta, fonte e destinazione, utilizzo; nonché di implementarne di ulteriori;

[257] Cfr E@H Data Model v 1.1 p. 9, 2015, disponibile alla risorsa: http://www.energy-home.it/Documents/Technical%20Specifications/E@h_data_model_v2.1.pdf

[258] In argomento, per gli indicatori quantitativi si rimanda al cap. 2 - *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità.*

[259] Cfr il parere Working Party ex art. 29 n. 223, 16 September 2014, Opinion 8/2014 *on the Recent Developments on the Internet of Things.*

iv. essere progettati per la raccolta, la registrazione e soprattutto il trasferimento *continuo*, *esteso* dei dati; quindi - in ragione all'interconnessione di cui al precedente punto ii), per la gestione e il trattamento della mole di dati collezionati;

v. funzionare in modalità *discreta*, *continua*, *pervasiva* - senza il più possibile ricorrere all'intervento o alla partecipazione dell'utente interessato.

Ogni oggetto *sensorizzat*o e connesso in rete capace di raccogliere, registrare e trasferire dati è un buon esempio di *IoT*[260]: gli esempi più consolidati si rintracciano in ambito *Wearable Computing* – con riferimento ad oggetti e accessori di abbigliamento; del *Quantified self* con attinenza a dispositivi indossati per misurare performance fisiche, sportive o di salute; della Domotica – con riferimento agli oggetti domestici (es: lavatrici, frigoriferi, forni) controllabili a distanza; o, ancora, in ambito *Smart Cities* e *Mobility* – per indicare ad esempio, dispositivi per il monitoraggio della mobilità e del traffico, la registrazione dei parametri di guida; in ambito *smart meetering* – con attinenza a contatori impiegati per misurare i consumi e indicatori energetici; ed ancora nei contesti della *Robotica,* dell'*Industria Biomedicale* e dell'*eHealth*.

Il ciclo di vita del flusso di dati di un servizio *IoT* prevede[261]:

i. la raccolta e la registrazione di *dati grezzi* nella misura e nel formato in cui sono stati raccolti, sostanzialmente privi di codifica o analisi; a titolo di esempio è possibile citare il numero di passi registrato da un contapassi;

ii. l'elaborazione di *dati aggregati* o *estratti* in termini di output ottenuto dai grezzi ed esplicativo di analisi comparative quantitative; un esempio - con riferimento al precedente punto, può essere rappresentato dal corrispondente andamento della velocità;

iii. la presentazione di *dati visualizzati* che saranno mostrati all'utente, ottenuti dai precedenti incrociandoli con indicatori di riferimento ed esplicativi di deduzioni quantitative più complesse o qualitative; rappresentano un possibile esempio (per rimanere nell'ambito di un contatore di *performance*) i report grafici sull'andamento nel tempo del livello di sforzo o delle calorie bruciate (dedotti con riferimento a soglie ed indicatori specifici) oppure previsioni sugli effetti dell'attività fisica (es. le calorie

[260] Per un ulteriore approfondimento sull'argomento, si indica: *Industry 4.0, Internet of Things, gli ambiti applicativi in Italia,* di Maurizio Bellini, 5 Novembre 2016 - illustra gli ambiti applicativi dell'*IoT* in Italia rilevate dall'Osservatorio del Politecnico di Milano in collaborazione con Digital4; disponibile alla risorsa: http://www.internet4things.it/iot-library/le-8-tecnologie-alla-base-dell-internet-of-things/

[261] Cfr Working Party ex art. 29 n. 223, 16 September 2014, Opinion 8/2014 *on the Recent Developments on the Internet of Things.*

bruciate, l'aumento delle prestazioni sportive o la perdita di peso).

Un diverso ma altrettanto significativo esempio può essere mutuato dalla fornitura di servizi di comunicazione ai quali possono essere associate deduzioni di profilazione: i metadati descrittivi i *log* di sistema relativi all'accesso (identificativo, data, ora, applicazione o dispositivo di rete, servizio richiesto) possono essere considerati *dati grezzi* che il fornitore di servizi può aggregare secondo parametri predefiniti (es. fascia oraria e durata di utilizzo del servizio richiesto) per ottenere, quindi, una catalogazione in *cluster* (dati aggregati) dell'insieme di utenti; catalogazione che può essere ulteriormente utilizzata per acquisire informazioni qualitative sul singolo utente (ad esempio l'interesse nel tempo verso un determinato servizio o prodotto) e, conseguentemente, consentire al fornitore di servizio di pianificare e ottimizzare strategie di marketing aziendale[262] e pubblicità comportamentale.

I servizi e le applicazioni di *IoT,* quindi, valutando ed incrociando i dati forniti dall'utente, con quelli di altri utenti, dell'ambiente e del contesto in cui si svolgono l'interazione e l'esperienza dei soggetti coinvolti, sono fortemente orientati alla estrazione di proprietà che lo riguardano e lo identificano; alla personalizzazione e alla profilazione rese sotto forma di servizi che semplificano la vita e la migliorano in termini di comodità, efficienza ed economicità. L'utente interessato - sotto la spinta dei vantaggi personali fruiti, è fortemente motivato a rilasciare e condividere pubblicamente i propri dati personali (specie se il rilascio è ulteriormente incoraggiato da compensazioni materiali, in denaro o premi)[263] senza però che ciò sia controbilanciato (in generale) da un pari interesse e preoccupazione ad essere informato e consapevole delle future e possibili implicazioni in termini di sfruttamento, ulteriore e diverso trattamento, protezione delle informazioni esposte.

I *dati* delle *cose* possono rivelare lo *stato* delle persone: da ciò consegue un forte rischio di auto-esposizione per l'utente (interessato) che consente al generico fornitore di servizi (qualificabile come titolare del trattamento[264]) di conoscere, accedere o dedurre una quantità di informazioni molto maggiore rispetto a quelle disponibili all'utente stesso[265].

---

[262] In argomento si cita il doc web n. 1629107/2009 emesso dal Garante Privacy in ordine agli adempimenti sui dati aggregati, *Prescrizioni ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione - 25 giugno 2009,* disponibile alla risorsa: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1629107

[263] *Con riferimento al precedente esempio attinente il progetto Energy@Home, potrebbe configurarsi la seguente situazione: l'utente in un'ottica di bilanciamento di business decide di esporre e condividere "quello che succede in casa": ad esempio il dato attinente il "numero di lavaggi della lavatrice". Questa informazione potrebbe essere utilizzata per ottimizzare i consumi e ricavare un risparmio in bolletta, ma al contempo e secondariamente, da questa informazione si potrebbero dedurre attitudini o comportamenti anche border-line.*

[264] Cfr GDPR art. 4 *Definizioni,* comma 7). *«titolare del trattamento»:la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

[265] Costituiscono esempi le seguenti possibili casistiche. a) Quando un utente condivide le informazioni sulla propria

All'attuazione dell'I*oT* concorre l'intervento combinato di molteplici attori che agiscono singolarmente o congiuntamente con distinti ruoli, diversi gradi di autonomia e di responsabilità: i fabbricanti dei dispositivi (i quali per primi ricevono i dati raccolti dagli oggetti *IoT*), gestori di piattaforme di dati, aggregatori o intermediari di dati, sviluppatori di applicazioni, piattaforme sociali, noleggiatori/noleggianti di dispositivi, gestori di piattaforme per l'*hosting* dei dati raccolti, ulteriori destinatari e organismi di normazione.

I portatori di interesse oltre a fornire all'utente funzionalità applicative *visibili* (*front-end*) delle quali l'utente è consapevole e al cui funzionamento ha acconsentito[266] possono accedere alle informazioni già archiviate nei dispositivi *IoT,* oppure riallocare quelle raccolte nei propri *Cloud* o nelle proprie piattaforme di *hosting* e *Data Mining* condividerle con attori terzi, senza che l'utente interessato ne sia a conoscenza o ne abbia compiuta consapevolezza.

La pluralità dei titolari del trattamento in combinazione con la intrinseca discreta (*silenziosa*, *invisibile*) pervasività di interconnessione informazionale dei dispositivi *IoT* – che implica una continua e *massiva* raccolta di informazioni limitando al minimo la partecipazione dell'utente interessato, risultano i più significativi presupposti di rischio per la *privacy* e la protezione dei dati personali in tale contesto.

In argomento non si riscontrano significativi esempi di implementazioni progettuali o operative volte a dotare gli oggetti e le infrastrutture *IoT* della nativa capacità di coinvolgimento del soggetto interessato resa, ad esempio, mediante l'*embedded* e l'esposizione di idonea informativa sul processamento dei dati raccolti o la configurazione di efficaci e validi strumenti di autorizzazione e consenso[267,268].

Al contempo, in argomento si evidenzia la mirata indicazione del Data Protection

---

posizione, raccolte dal proprio smartphone e trasferite a piattaforme sociali (es. Facebook), queste ultime possono analizzare i dati nel tempo, estrarre ricorrenze e proporre all'utente suggerimenti su eventi locali, offerte, o presenza di contatti e amici. *Cfr* https://it-it.facebook.com/about/privacy *- normativa sui dati di Facebook e su come Facebook utilizza le informazioni raccolte;* b) i dati registrati da un contapassi e trasferiti al fabbricante del dispositivo possono essere convertiti in livelli di stress fisico, confrontati con i battiti cardiaci (per esempio) e se analizzati nel tempo possono produrre report sugli effetti dell'attività e delle performances ma anche anticipare eventuali problemi di salute o predisposizione ad alcune patologie; c) Se, inoltre, l'utente condivide questi dati con piattaforme sociali, queste possono trattarli per finalità diverse: dedurre che l'utente pratica costantemente attività fisica e proporre pubblicità di articoli sportivi.

[266] A titolo di esempio si citano le interfacce Web di raccolta e visione dei dati collezionati, o le interfacce accessorie di controllo e di gestione base delle *preferences* di *privacy*.

[267] Cfr: Sadeghi A., Wachsmann C., Waidner M., *Security and privacy challenges in industrial Internet of Things,*(2015)

Abomhara M., Koien Geir M., *Security and privacy in the Internet of Things: Current status and open issues* (2015)

Whitmore A., Agarwal A., Da Xu L., *The Internet of Things—A survey of topics and trends, Information Systems Frontiers,* Volume 17, Issue 2, pp 261–274 (2015)

Sicari S., Cappiello C., De Pellegrini F., Miorandi D., Coen-Porisini A., *A security-and quality-aware system architecture for Internet of Things,* Information Systems Frontiers, Volume 18, Issue 4, pp 665–677 (2016)

[268] Per la definizione e le proprietà del consenso si rimanda al cap. 1 - *Lo scenario normativo attuale. questioni aperte.* Paragrafo 3. *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: le principali novità.* – 4. *Il Regolamento Generale sulla protezione dei dati (UE) 2016/679: il soggetto interessato e il dato personale.*

Working Party art. 29 contenuta nel parere n. 223/2014 volta a sostenere un nuovo utilizzo delle *Sticky Privacy Policies* e *Privacy Proxies*[269] quale meccanismi atti a responsabilizzare l'interessato nella gestione del consenso attraverso gli oggetti stessi.

Le indicazioni del WP, per entrambi gli strumenti sono consultabili alla pagina 23 del documento, che per quel che attiene le *Sticky Privacy Policies* riporta:

> *<l'uso di un approccio basato sulle cosiddette sticky policies può favorire la conformità al quadro giuridico in materia di protezione dei dati in quanto prevede di integrare le informazioni sulle condizioni e i limiti d'uso dei dati nei dati stessi. Pertanto, tali politiche potrebbero definire il contesto di utilizzo dei dati, le finalità, le politiche riguardanti l'accesso di terzi e una lista di utenti fidati>;*

ed in attinenza ai *Privacy Proxies,* indica:

> *<Un modo che consenta di offrire all'interessato il controllo reale sul trattamento dei dati quando interagiscono con i sensori offrendogli anche la possibilità di esprimere preferenze, di ottenere o revocare il consenso e di limitare le finalità, potrebbe essere basato sull'uso di privacy proxies. Con l'aiuto di un dispositivo le richieste di dati vengono confrontate con politiche predefinite che regolano l'accesso ai dati sotto il controllo dell'interessato. Tramite la definizione di coppie formate da un sensore e una politica, le richieste di terzi di raccogliere o accedere ai dati dei sensori verrebbero autorizzate, limitate o semplicemente respinte>.*

Pur con le dovute limitazioni i dati generati dalle cose e descrittivi delle cose concorrono a comporre il volume e la varietà dei *Big Data,* e se considerati in una prospettiva semantica, ad essere trattati secondo lo *schema Big Data;* questo argomento sarà illustrato e approfondito nel successivo paragrafo 1.3. "*Big Data" e Data Mining*.

[269] Per quel che attiene le *Sticky Privacy Policies* e i *Privacy Proxies* si rimanda al cap. 3 - *Privacy e Protezione dei Dati personali: le contromisure*, Paragrafo 2.4. *Le Privacy Policies di tipo "User-centric" e "Data-centric". Sticky Privacy Policies. Privacy Proxies*

1.2. *APPS* PER *SMART-DEVICES.*

Le *apps* sono applicazioni software tipicamente sviluppate per un compito specifico e destinate a una serie particolare di dispositivi *intelligenti* (interconnessi): smartphone, tablet e televisori connessi a Internet. Le *apps* elaborano le informazioni in modo compatibile alle caratteristiche specifiche del dispositivo, interagendo strettamente con l'hardware e il sistema operativo montati su di esso (quindi tipicamente si distinguono apps per *Android,* oppure apps per *iOS*[270]).

I sistemi operativi mobili sono progettati per esporre specifiche funzionalità di accesso per il tramite di *API* (*Application Programming Interface).* L'accesso può essere diretto a sensori - ad esempio di prossimità, di audio/video integrati nella fotocamera, oppure al giroscopio, alla bussola o all'accelerometro; ad interfacce di rete – quali ad esempio *Wi-Fi, Bluetooth, NFC;* oppure a servizi e strutture dati nativi – quali ad esempio il calendario, la rubrica dei contatti.

Grazie a queste *API* gli sviluppatori di *apps* possono accedere alla memoria e al sistema operativo del dispositivo per raccogliere, modificare, cancellare, inviare dati; modificare le impostazioni del dispositivo; acquisire dati univoci dello stesso (e quindi identificativi dell'utilizzatore) quali ad esempio numero di cellulare o codici *IMEI, IMSI, UDID.*

La *apps* possono, quindi, assimilarsi alle tradizionali applicazioni software scritte ed eseguite in compatibilità ad un sistema operativo installato sul personal computer, per il tramite di un ambiente di sviluppo di *SDK – Software Developmet Kit,* con la differenza di essere caratterizzate una semplificazione e un approccio implementativo a basso livello, volto ad ottenere leggerezza, essenzialità e velocità, in linea con le limitate risorse hardware dei dispositivi mobili rispetto agli ambienti desktop.

Le *apps* si suddividono in *apps native, web apps, apps ibride*[271]. Le *apps native,* sono scaricate, installate ed eseguite interamente nel dispositivo mobile, e quindi mirate allo specifico sistema operativo, sviluppate nel codice nativo dello stesso[272]; la capacità elaborativa e computazionale del dispositivo sono essenziali al funzionamento dell'*app;* le *apps* native sono rilasciate da un

---

[270] *Android e iOS,* sono i principali sistemi operativi mobili (OS) oltre a: Windows Phone, Symbian, Blackberry 10 (QNX); ed altri meno diffusi o in disuso, quali Bada e dei sistemi GNU/Linux, embedded come Embedded Linux, Tizen (successore di LiMo e MeeGo), Sailfish OS, Maemo, MeeGo, Ångström, Ubuntu Touch/Ubuntu Phone, Firefox OS, Open webOS, Openmoko, ed altri.
Cfr https://it.wikipedia.org/wiki/Smartphone

[271] In argomento per i dettagli si rimanda ai seguenti articoli:
Mobile Apps, di Giulio Roggero *I parte: Applicazioni mobili, un mercato maturo e in crescita,* (Febbraio 2014)
http://www.mokabyte.it/2014/02/mobileapps2014-1/
II parte: Trend e tecnologie. Pro e contro delle app native e ibride, (Aprile 2014)
http://www.mokabyte.it/2014/04/mobileapps2014-2/

[272] Ne sono esempio: *Objective-C* per *iOS* e *Java* per *Android.*

app store dedicato. L'interazione diretta con le API messe a disposizione dal costruttore del sistema operativo garantirà accesso immediato a tutte le funzionalità del dispositivo oltre a permettere prestazioni ottimali e migliorarne l'usabilità. Questa tipologia di *apps* ampliano, quindi, le caratteristiche native del dispositivo incluse all'interno del sistema operativo, estendendo e personalizzandone le funzioni *embedded* native.

In un contesto desktop le *apps native* sono sovrapponibili alle tradizionali applicazioni eseguibili su personal computer (in genere rilasciate in formato eseguibile, distinto dall'estensione *.exe)*.

Le *web apps* consistono in un collegamento verso un applicativo remoto - implementato in un linguaggio cross-platform (ad esempio HTML5), per il tramite di un livello software di interfaccia distinto, allocato sul dispositivo mobile o anch'esso su un server remoto: in pratica l'*app gira* e viene fruita all'interno di un *runtime custom* contenuto nel web browser del dispositivo.

Questa soluzione comporta importanti conseguenze in termini di funzionamento: il vantaggio principale di una *web app* consiste nel fatto di non incidere se non minimamente sulle capacità di memoria e di calcolo del dispositivo in quanto il nucleo elaborativo e/o l'interfaccia utente dell'applicazione sono collocati su server remoti; ulteriore vantaggio delle *web apps* è quello di poterle rilasciare come un sito web senza passare dallo store e quindi essere indipendente dal *vendor;* al contempo le *web apps* sono fruibili da tutti i web browser desktop.

Di contro il funzionamento di una *web app* richiede il costante accesso a internet, le sue prestazioni dipenderanno strettamente dalla velocità di connessione, presentando comunque negazioni di accesso a molti dei sensori hardware del device, per limitazioni esposte dalla *sandbox* del web browser.

In un contesto desktop le *web apps* sono sovrapponibili alle tradizionali applicazioni eseguibili nei web browser, nativamente o per il tramite di *plug-in*.

Le *apps ibride* girano all'interno di un *runtime custom* che contiene una *web view* (analogo al web browser delle *web apps*). Il runtime espone questa web view con APIs che "avvolgono" quelle del dispositivo mobile ed espongono le proprie in JavaScript. È quindi sufficiente invocare queste APIs e dalla web view per poter accedere all'hardware del dispositivo come, ad esempio l'accelerometro, i contatti o la fotocamera del telefono, funzionalità proibite da un web browser normale. Questo approccio rimane svincolato dallo store e dal vendor per se non per l'SDK (in ragione dell'utilizzo di HTML5 implementante il *wrapper*), con delle performance

intermedie tra le *apps* native (in assoluto più efficienti) e le *web apps*.

In un contesto desktop le *apps* ibride sono sovrapponibili alle *java applet* o *active-x* eseguibili tramite i corrispondenti *runtime environment*.

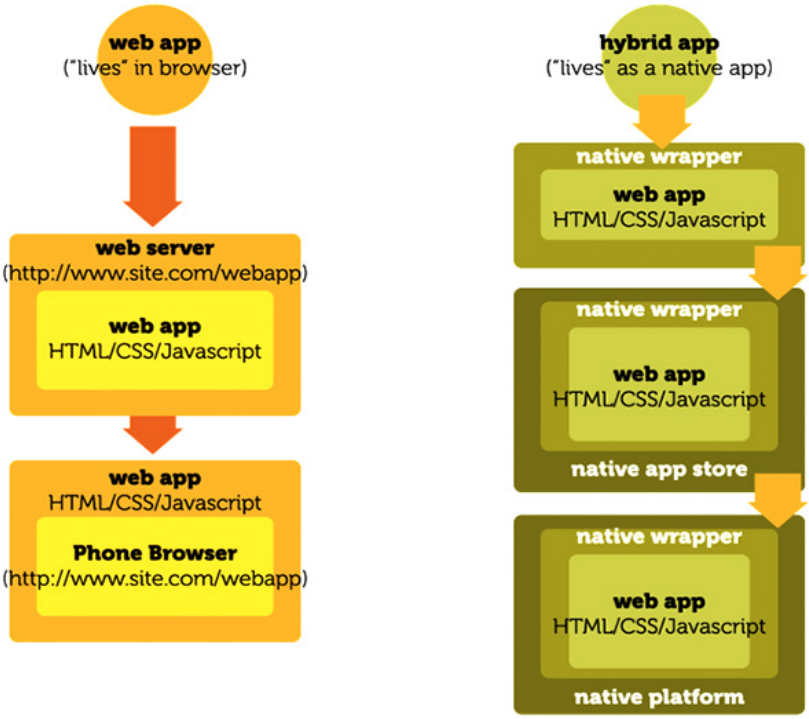


Figura 4.3 - Confronto tra *web apps* e *apps ibride*[273].

Le applicazioni e i servizi resi dalle *apps* sono numerosissime e variano per tipologia, esponendo funzioni di navigazione Internet e comunicazione (e-mail, messaggistica, telefonia); intrattenimento (giochi, film/audio, musica), lettura di quotidiani e news; phone-banking, servizi finanziari; negozi virtuali e servizi di retail; geolocalizzazione di persone, mezzi di trasporto; misurazione di performance fisiche; sportive; gestione degli indicatori di salute; servizi pubblicitari contestuali o personalizzati.

Le *apps* vengono offerte all'utente finale gratuitamente o a un costo minimo, la base di utilizzatori può variare da pochi individui a molti milioni. Secondo un report pubblicato da *IDC – Internation Data Corporation*[274], nel 2015 sono state installate circa 156 miliardi di *apps* per un guadagno diretto pari a circa 34,2 miliardi di dollari e con una previsione per il 2020 di 210 miliardi di installazioni all'anno e un guadagno diretto stimato in 57 miliardi di dollari.

[273] Cfr http://www.mokabyte.it/2014/04/mobileapps2014-2/

[274] Per un maggior dettaglio si rimanda alla risorsa disponibile su http://www.pcprofessionale.it/blog/mercato-app/, e all'articolo *I numeri del mercato delle app - Google Play genera il maggior numero di download, ma è l'App Store di Apple che crea il maggior guadagno diretto,* di Michele Braga, 10 Maggio 2016.

I principali attori coinvolti nello sviluppo, nella distribuzione e nella gestione delle *apps* sono quattro[275], e comprendono:

i. gli sviluppatori di applicazioni: creano apps e/o le mettono a disposizione di utenti finali. La categoria comprende aziende del settore privato o organizzazioni del settore pubblico che commissionano lo sviluppo di applicazioni, le società o le persone fisiche che creano e lanciano applicazioni. Progettando e/o creando il software che girerà sugli smartphone, gli sviluppatori discriminano in che misura l'applicazione potrà accedere a diverse categorie informazioni e procedere al loro processamento sia nel dispositivo che attraverso risorse informatiche remote;

ii. i produttori di sistemi operativi e di dispositivi: rispetto al funzionamento e alla gestione delle apps il loro ruolo attiene principalmente l'esposizione delle *APIs,* e l'implementazione delle funzionalità di sicurezza, in particolare quelle di tipo *privacy by design;*

iii. gli *app store:* provvedono alla distribuzione e alla commercializzazione delle apps; tipicamente sono associati e vincolati a un sistema operativo, anche se parallelamente alla loro diffusione le apps sono reperibili direttamente dai siti di coloro che le sviluppano, dalle aziende o qualsiasi privato che voglia mettere a disposizione una propria applicazione;

iv. terze parti coinvolte nell'ambito dell'utilizzo, dei servizi e nei prodotti erogati dalle *apps:* in questo gruppo rientrano parti coinvolte in servizi considerabili accessori per tipologia ma non per rilevanza o diffusione; rappresentano esempi i fornitori intermediari per prodotti di pubblicità contestuale o personalizzata, oppure per i servizi trasversali di tracciamento e marcatura del dispositivo tramite *cookies,* od ancora per servizi analitici degli indicatori di utilizzo, popolarità e fruibilità delle *apps.*

La stretta e silenziosa interazione con il sistema operativo consente alle *apps* di accedere ad un numero notevolmente maggiore di dati rispetto a un browser o navigatore tradizionale, abilitandole a raccogliere grandi quantità di informazioni, di elaborarle per fornire servizi accessori e innovativi all'utente finale. Molte delle informazioni accedute e trattate sono dati personali, identificativi, informazioni private che concernono non solo il proprietario del dispositivo ma anche altri utenti (si pensi ad esempio ad immagini, video o ai contatti inclusi nella rubrica).

[275] In argomento si indica il parere Working Party ex art. 29 n. 202, 27 Febbraio 2013, Opinion 2/2013 *on apps on smart devices*

Tuttavia, le stesse fonti di dati possono essere ulteriormente elaborate, di solito per generare un flusso di entrate, con modalità che possono essere ignorate o indesiderate dall'utente finale rappresentando quindi tanto un fattore di vulnerabilità, tanto significative implicazioni di rischio per la *privacy* e la protezione dei dati personali.

In analogia all'*IoT* i dati generati dalle *Apps* concorrono a comporre il volume e la varietà dei *Big Data,* e se considerati in una prospettiva semantica, ad essere trattati secondo lo *schema Big Data;* questo argomento sarà illustrato e approfondito nel seguente paragrafo 1.3. "*Big Data" e Data Mining*.

1.3. "*BIG DATA*" E *DATA MINING.*

Big Data è l'insieme di dati che si caratterizza per il Volume, la Velocità e la Varietà[276] con cui vengono generati e prodotti; modello che - parallelamente all'evoluzione del fenomeno, è possibile perfezionare con ulteriori 3V: Veridicità, Variabilità e Valore[277] descrittive di altrettante proprietà. Una infografica rilasciata da IBM[278] rappresenta molto bene il fenomeno Big Data, in termini delle 4V – Volume, Velocità, Varietà e Veridicità (Veracità).

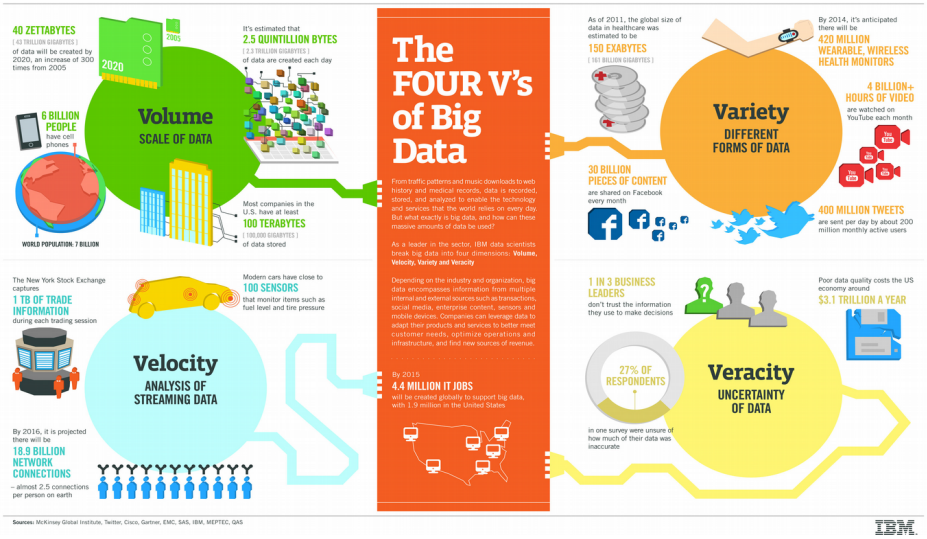


Figura 4.4 – Big Data e il paradigma delle 4 V: Volume, Velocità, Varietà e Veracità

La prima *V-Volume* rappresenta un indicatore quantitativo riconducibile sia alla crescente disponibilità di dati prodotti in rete[279], sia alla facilità e soprattutto alla sempre maggiore economicità di raccolta e di analisi. La crescente disponibilità di dati digitali unitamente alla maggior potenza tanto di *storage* quanto elaborativa derivante dall'interconnessione di *devices* (computer, smartphone, tablet...) con infrastrutture *Cloud,* permette di analizzare qualsiasi fenomeno (economico, sociale, scientifico, ...) nella sua interezza e globalità potendo contare non più solo su in ristretto campione rappresentativo ma sull'intero dominio di dati raccolti e relativi lo specifico fenomeno.

La seconda *V-velocità* rappresenta anch'essa un indicatore quantitativo, attiene il fatto che

[276] Il c.d paradigma delle 3V.

[277] Sull'introduzione delle ulteriori due V - Variabilità e Valore, si rimanda agli atti del convegno Italy/Usa Meeting A new model of education and research for the digital health development, specificatamente al contributo del dott. Luca Sangiorgi, IOR – Istituto Ortopedico Rizzoli Bologna in tema di Big Data for Healthcare.

[278] La risorsa è disponibile su: http://www.ibmbigdatahub.com/infographic/four-vs-big-data.

[279] La quantità di informazioni digitali disponibili cresce ad un ritmo esponenziale: entro il 2020 si stimano 450 Mln transazioni giornaliere B2B e B2C su Internet e 24 Mld device connessi in rete. In argomento, per ulteriori indicatori quantitativi si rimanda al cap. 2 - Privacy e Protezione dei Dati personali: pluralità semantiche e criticità, paragrafo 1 – I dati e le informazioni personali.

i dati digitali vengono prodotti dinamicamente per flussi e stream continui di informazioni che implicano – in tempo reale, aggiornate e non differibili elaborazioni sulla base di rinnovati dati.

La terza *V-Varietà* rappresenta un indicatore qualitativo, riconducibile alla varietà di forme e di formati con cui vengono prodotti i dati: documenti, testi, post o applicazioni pubblicati o esposte sui social media; file word, pdf; immagini e video rilasciati da videocamere e fotocamere digitali; dati di connettività, di geolocalizzazione GPS; informazioni scambiate tramite mobile (smartphone, tablet), SMS e chat di messaggistica; ed inoltre dati prodotti da fidelity card, distributori automatici, sensori, transiti in aeroporto, tracking, pacchi; etc). La *Varietà,* quindi, misura la complessità connessa all'estrema eterogeneità delle fonti dei dati e alla difficoltà di collegare dati con provenienze differenti.

L'informazione Big Data è quindi intrinsecamente variegata ed eterogenea; questo apre al quarto indicatore tipicamente qualitativo: *V-Veridicità*[280] parametro ricompreso nel più ampio spettro di qualità dei dati; la varietà dei *Big Data* e la diversità delle fonti rende molto difficile provarne la correttezza, l'attendibilità, l'affidabilità. Maggiore è la velocità di produzione e di raccolta dei dati, maggiore è il volume, maggiore la complessità e la varietà, minime la correttezza, la veridicità, la qualità nel suo complesso.

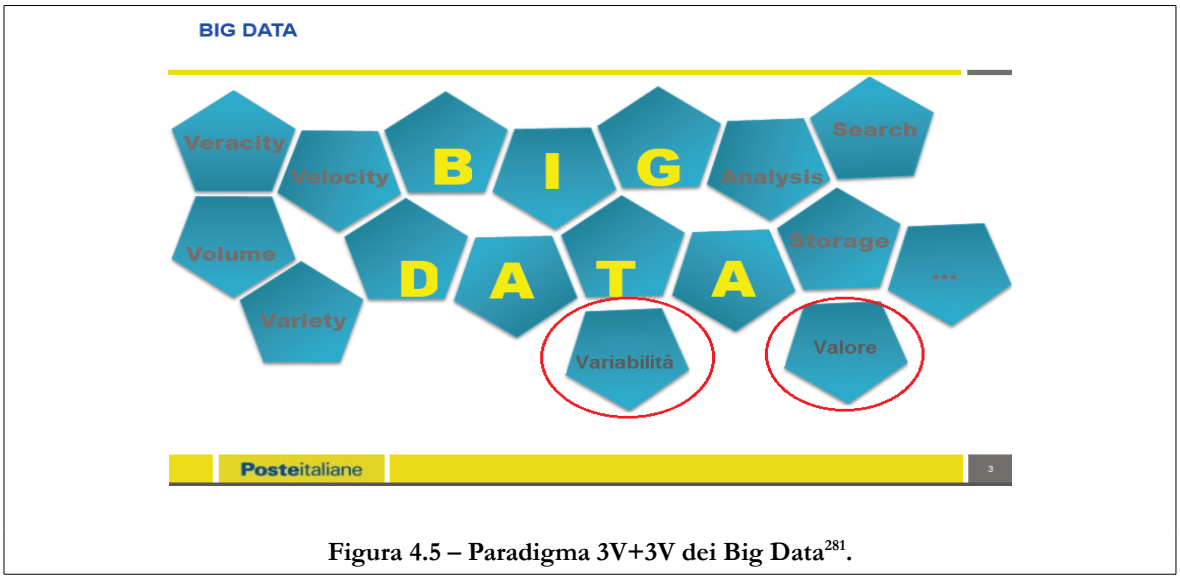


Figura 4.5 – Paradigma 3V+3V dei Big Data[281].

La *V-variabilità*[282], è un indicatore quantitativo volto a misurare la discontinuità di

[280] Questo parametro è stato introdotto a IBM, per misurare la dimensione della inaffidabilità dei dati in un contesto di 3VBig Data. Per un maggiore approfondimento si indica la seguente risorsa: https://www.oranjob.com/academy/big-data-e-la-previsione-del-futuro/

[281] Infografica tratta e modificata da un contributo di Poste Italiane - BIG DATA & CYBERSECURITY, presentato dall'Avv. Alessandra Toma alla 6ª edizione Privacy Day Forum organizzato da FederPrivacy e tenutosi a Roma il 13 Ottobre 2016.

[282] Questo parametro è stato introdotto da SAS, per misurare la dimensione della complessità dei dati in un contesto di 3VBig Data. Per un maggiore approfondimento si indica la seguente risorsa: https://www.oranjob.com/academy/big-

produzione dei *Big Data,* rilasciati in volumi e periodi temporali non costanti. Unitamente alla *Varietà* misura il grado di complessità e in-consistenza dei *Big Data.*

La *V-Valore*[283]*,* è un indicatore sia qualitativo che quantitativo, è volto a misurare l'indice di sfruttabilità dei *Big Data* nelle tre fasi di processamento che presentano caratteristiche sovrapponibili a quelle illustrate al precedente paragrafo per il contesto informazionale dell'*Internet of Things:*[284] in forma grezza i Big Data presentano un basso e scarso valore, che aumenta proporzionalmente all'elaborazione con il passaggio in forma semistrutturata e aggregata, quindi nel successivo stadio di dati strutturati e visualizzati. Il valore è inoltre un indicatore strettamente connesso alla veridicità, essendo il (ri)utilizzo conseguenziale alla possibilità di valutare, comprendere e dimostrarne l'attendibilità e l'affidabilità.

Ma qual è l'innovativo significato del termine *Big* dei *Big Data?* La risposta si colloca nella differenza tra il "cercare" e il "trovare" una risorsa, un contenuto, una informazione in Internet. L'ampiezza dei *Big Data* punta a incrociare la dimensione quantitativa e quella qualitativa del dato, nella misura un cui algoritmi sono sempre più in grado di *comprendere* il dato, *estrarre* e le relazioni semantiche con gli altri dati, ricavare nuova informazione mediante attributi ritenuti pertinenti e attendibili (componente qualitativa), all'interno di una mole crescente di dati (componente quantitativa). Questo concetto è efficacemente rappresentato dall'espressione *schema Big Data*[285]: un meccanismo di arricchimento dei dati.

La rete di interconnessione degli oggetti informazionali presenti in Internet è – al momento, ancora frutto di decisioni unilaterali di chi pubblica tali risorse: l'*uploader* decide di collegare (e rimandare) le risorse pubblicate ad ulteriori, ritenute pertinenti. I motori di ricerca lavorano proprio su questo meccanismo di rimandi e di collegamenti formati dagli *hyperlink;* essi classificano l'informazione ricercabile sulla base di indicatori di posizionamento pesati dal numero di *hyperlink* entranti e dal numero di visite[286]; un meccanismo di classificazione delle risorse - distribuito e determinato dalla totalità degli utenti del web, dalla frequenza e dalla numerosità delle loro visite nonché base dell'algoritmo *PageRank,* che ha reso possibile a Google di implementare il processo più efficiente e attualmente in uso di *cercare*

data-e-la-previsione-del-futuro/

283 Questo parametro è stato introdotto a ORACLE, per misurare la dimensione della complessità dei dati in un contesto di 3VBig Data. Per un maggiore approfondimento si indica la seguente risorsa: https://www.oranjob.com/academy/big-data-e-la-previsione-del-futuro/

284 Il ciclo di vita del flusso di d Big Data comprende: dati in forma grezza, aggregata e visualizzata.

285 Cfr D'Acquisto G., Naldi M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017) p. 10-20

286 Si tratta della c.d *saggezza della folla* (*wisdom of the crowd*).

un'informazione sul web.

Il successivo passaggio di *trovare* l'informazione desiderata è totalmente a carico di chi la richiede[287]: il motore (di tipo *search-engine) cerca* l'utente valuta e *trova.*

Lo *schema Big Data* può ribaltare questo passaggio in ragione della grandezza dei dati da intendersi non tanto (o esclusivamente) come *più quantità di dati,* ma come ampliato volume di influenza e associabilità a fenomeni, situazioni, eventi.

In questo senso è possibile pensare ai *Big Data* come evoluzione del semantic web (web 2.0), e il (Big) dato (anche il più piccolo e apparentemente insignificante) come risultante di attributi descrittori ad esso associati: maggiore, più pertinente, adeguato ed efficace sarà il numero di questi descrittori più probabile e significativo sarà il collegamento con altri dati (a loro volta descritti da ulteriori attributi), quindi più ampia e più qualitativa la tipologia di connessioni semantiche tra risorse informazionali, più attendibile la relazione tra fenomeni.

Il collegamento tra due dati sarà costruito in termini di intersezione dello stesso subset di attributi. In uno "schema *Big Data*" il motore di ricerca evolve dall'essere *"search-engine"* (associato a schemi *Smart Data*) a *"find-engine"* (associato a schemi *Big Data),* quest'ultimo si distingue per essere capace di trovare nuovi dati (in esito di queries di ricerca) tramite misure di correlazione e valutazioni incrociate sull'affinità semantica degli attributi descrittori.

Questo passaggio è esemplificato con un esempio: supponiamo di voler rilasciare, pubblicare e condividere in rete due semplici risorse informazionali, due dati: *Varietà* e *Volume.*

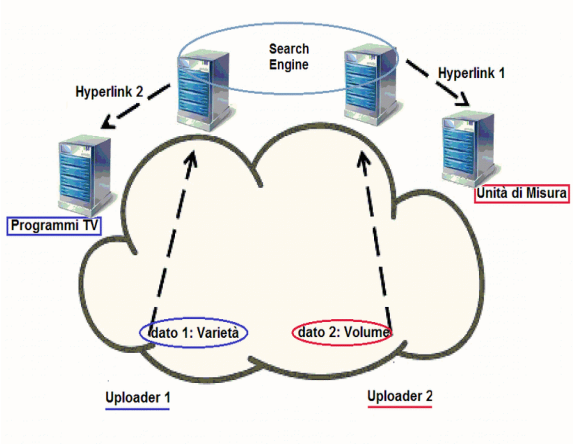
In modalità *Smart Data* i due dati *Varietà* e *Volume* sono caricati separatamente su due server, e altrettanto separatamente collegati ad rispettivi domini (es. "Programmi TV", e "Unità di Misura"). Il motore di ricerca *(search engine)* - in esito al *wisdom of the crowd,* indicizza separatamente i due dati, nei rispetti circuiti. Il passaggio di ulteriore ricerca per il recupero dell'associazione richiesta, e per trovare quindi l'informazione desiderata, è a carico di chi effettua la ricerca.

Diversamente, in modalità *Big Data,* il motore di ricerca *(find engine)* applicando diverse possibili tecniche di *processing*[288] estrae – per entrambi i dati di partenza, una serie di descrittori cercando ogni possibile corrispondenza semantica tra questi e i descrittori di altri dati: il

[287] Cfr D'Acquisto G., Naldi M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017) p. 9

[288] In letteratura esistono diverse tecniche per l'estrazione di descrittori; alcune sono di natura passiva (effettuate in modo automatico senza l'intervento umano), tra queste rientrano: il *machine learning,* l'*hashing,* la *trasformata di fourier,* concordanze e stilometria; altre di natura attiva (effettuate con l'intervento umano perché basate sul significato e la semantica dei descrittori), tra queste rientrano: la classificazione semantica e il *crowdsourcing.*

risultato consiste in nuovi descrittori e in nuove corrispondenze esposte direttamente dal motore di ricerca; nell'esempio queste corrispondenze sono rappresentate dalla risorsa informazionale *Big Data* e dall'insieme degli articoli di ricerca sul tema *Big Data.*



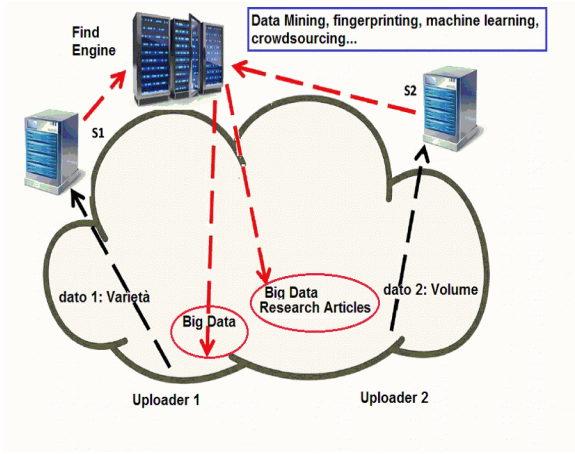


Figura 4.6 – Contesti *Smart Data* e *Big Data*[289]

Nei contesti *Smart Data* i collegamenti *(hyperlink)* sono a priori fissati da chi ha caricato la risorsa in rete; il criterio per determinare l'ordine dei risultati di una query di ricerca è esclusivamente quantitativo: il motore di ricerca *Search Engine* conta il numero delle visite per misurare le connessioni tra il dato richiesto e gli altri dati, e quindi per posizionarne gli esiti. Nei contesti *Big Data* il criterio per determinare le connessioni tra i dati è qualitativo: il motore di ricerca *Find Engine* correla i dati intersecando le occorrenze congiunte, formula la priorità dei collegamenti e delle relazioni tra le risorse informazionali valutando la maggiore affinità semantica tra i descrittori esposti ed estratti dai dati, quindi deduce e inferisce nuove relazioni, nuovi collegamenti, nuova informazione.

Il passaggio dai motori di ricerca *search engine - web 1.0* a *find engine - web 2.0* in qualche misura è già in atto ed attiene ad esempio il completamento automatico delle queries di ricerca e la disambiguazione dei risultati, la possibilità di effettuare ricerche per immagini o per suoni; questo scenario evolverà sempre più verso contesti di realtà aumentata[290] grazie alla potenzialità dello "*schema Big Data*": quantitativo nella cardinalità del dominio dei descrittori e qualitativo nei loro requisiti di efficacia[291].

Il mantenimento di questi requisiti evolverà e perfezionerà il *find engine* integrandolo senza discontinuità alla *user-experience* dell'utente, il quale quindi potrà apprezzare i benefici della personalizzazione e, se in linea con le proprie aspettative, percepire i suggerimenti confezionati

[289] Gli esempi citati sono stati mutuati per immagini e descrizione da: D'Acquisto G., Naldi M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017) p. 11-13

[290] Se si pensa di sovrapporre alla fitta rete di *hyperlink* già presenti in rete lo schema Big Data, questo consentirà per esempio di conoscere in quale luogo è stata scattata una foto; il soggetto ritratto in un dipinto, il suo autore, la attuale collocazione in musei; gli eventi associabili ad un luogo; ad una mappa la presenza di servizi accessori presenti sul percorso; la filmografia o la discografia relazionate ad un tema; all'immagine di un volto anonimo i dati identificativi (nome, cognome, profilo social....). Il dettaglio di questo argomento si rimanda la prossimo paragrafo 1.4 – Realtà Aumentata e *Data Accretion*

[291] Cfr successivo paragrafo 3 - *La garanzia di qualità dei dati e le nuove tipologie di rischio per la Privacy*

ritenendoli familiari e tutt'altro che fastidiosi. A ciò concorrerà la capacità di analizzare l'andamento storico delle abitudini d'uso degli utenti nei vari servizi e la possibilità di categorizzare profili a cui mirare le proposte con elevata probabilità di successo.

Da ciò consegue che l'ampliamento semantico dei *Big Data* – la cui potenza è quindi sostanzialmente descrittiva, sarebbe impensabile senza l'utilizzo e il processamento di informazioni personali (iniziali e nuove) per scopi e finalità che non possono mantenersi fissate su quelle iniziali: è praticamente impossibile pensare che un trattamento *Big Data* possa restare confinato ad una sola finalità o riguardare costantemente e soltanto gli scopi previsti al momento della raccolta acconsentiti dal soggetto interessato.

I trattamenti attuati con tecniche di *Big Data* hanno ad oggetto dati personali non solo legittimamente trattati sulla base del consenso informato rilasciato dagli utenti, ma anche collezionati da fonti *open source;* coinvolgono informazioni relativi a persone identificate o identificabili recuperate in rete da fonti pubbliche[292]; rilasciate dagli stessi utenti nelle più svariate forme della loro *on line experience,* ed in particolare quella attinente la pubblicazione di immagini, post e contenuti personali su profili pubblici di social network; prodotte da oggetti *IoT* e rese pubbliche dagli stessi utenti.

La intrinseca massimizzazione delle informazioni personali utilizzate, il mantenimento dei requisiti di qualità dei dati (veridicità), l'impossibilità di configurare nel tempo le finalità di trattamento secondarie e, quindi, di mantenerne il presupposto di liceità vincolato alle condizioni di consenso, rappresentano notevoli criticità per la protezione dei dati nel trattamento *Big Data.*

[292] Ad esempio ricavate esercitando il diritto di accesso o in esito degli adempimenti di trasparenza posti in essere dalle pubbliche amministrazioni.

1.4. REALTÀ AUMENTATA E *DATA ACCRETION*

Minority Report è un film del 2002 diretto da Steven Spielberg, liberamente tratto dall'omonimo racconto di fantascienza di Philip K. Dick. *Nel 2054 la città di Washington ha cancellato gli omicidi da ormai 6 anni grazie a un sistema chiamato PreCrime. Basandosi sulle premonizioni di tre individui dotati di poteri extrasensoriali di precognizione amplificati, detti Precog, la polizia riesce a impedire gli omicidi prima che essi avvengano e ad arrestare i potenziali "colpevoli". In questo modo non viene punito il fatto (che non avviene), bensì l'intenzione di compierlo e che porterebbe a concretizzarlo: è un sistema delicato, osteggiato da molti, che però sembra funzionare senza intoppi*[293].

In chiusura oggetti *IoT* intercettano e localizzano il movimento di uno dei protagonisti - John Anderton (interpretato da Tom Cruise); *on the fly,* lo identificano, individuano ed estraggono alcune sue caratteristiche fisiche (ad esempio l'iride, il volto, l'odore) e, sulla base di queste, in tempo reale chiamandolo per nome propongono proposte personalizzate per l'acquisto di un nuovo modello di macchina, di un nuovo profumo, di regali per i suoi amici; prodotti mirati, familiari, adatti alle esigenze e alla personalità del soggetto al quale vengono indirizzate.

Per quanto avveniristico questo è un buon esempio di realtà aumentata. Altri esempi meno visionari possono essere l'aumento descrittivo dell'immagine di un bene culturale identificato per geolocalizzazione e arricchito di informazioni storiche o artistiche; oppure l'ampliamento sonoro della materialità di un oggetto *parlante* dei suoi possibili utilizzi o rivelatore dello stato di usura o di malfunzionamento.

Per realtà aumentata, si intende - di base, il miglioramento della percezione sensoriale umana mediante informazioni, in genere manipolate e convogliate digitalmente, non altrimenti o naturalmente percepibili o disponibili. Gli elementi che *aumentano* la realtà possono essere aggiunti attraverso un dispositivo mobile, come uno smartphone, oppure con l'utilizzo di un personal computer dotato di webcam, oppure con altre tipologie di sensori montati su videocamere digitali o rilevatori, od ancora mediante dispositivi di visione (per es. occhiali a proiezione sulla retina), di ascolto (auricolari) e di manipolazione (guanti)[294].

Il miglioramento della realtà può avvenire sia per aumento ed arricchimento delle informazioni, sia per diminuzione ed eliminazione dell'informazione non utile. L'arricchimento di informazione desta molte e non banali questioni rispetto al soggetto

[293] Cft https://it.wikipedia.org/wiki/Minority_Report
[294] Cfr https://it.wikipedia.org/wiki/Realt%C3%A0_aumentata

interessato e fruitore, il quale se per un verso può considerare l'aumento della realtà osservata come un beneficio e sfruttarne i vantaggi derivanti dall'ampliamento di conoscenza, per un altro potrebbe percepirne l'impatto anche come un'azione invasiva veicolo di un contenuto informativo, in definitiva, non desiderato; valutare con fastidio che un *oggetto* – in un determinato contesto, sia in possesso di informazioni senza averle volontariamente e reciprocamente condivise.

Le implicazioni di *scontestualizzazione* della realtà diventano più critiche quando un dato digitale viene arricchito con informazioni personali, quindi associabili ad una persona, con conseguenti ricadute di identificazione diretta o indiretta.

Sull'argomento al fine di significare l'impatto della realtà aumentata, rispetto alla protezione dei dati personali, si riportano le sperimentazioni di re-identificazione svolte nell'ambito di uno studio condotto nel 2014 dal gruppo di ricerca del prof. Alessandro Acquisti[295] presso la Carnegie Mellon University (Pittsburgh, Pennsylvania USA). Questo studio si colloca in contesti informazionali alimentati con dati personali pubblicati volontariamente sul proprio profilo Facebook dagli stessi soggetti interessati.

A premessa, rispetto alla sperimentazione, si indicano due *trend* paralleli di contesto e importanti in qualsiasi applicazione di realtà aumentata: il primo attiene la costante ed enorme crescita di foto pubblicate sui social ed in particolare su Facebook[296] buona parte delle quali, grazie al meccanismo del *tagging*, risultano associate a dati personali identificativi (nome e cognome) del soggetto interessato; il secondo attiene la crescente capacità elaborativa dei sistemi di *face recognizer* per il successo delle operazioni di *face detection* e *face identification*[297].

A ciò si aggiunga un fattore esogeno rispetto all'utente connesso ai *default settings* di Facebook di trattare l'immagine del profilo (la *primary profile photo)* come dato obbligatorio e pubblico, con associati nome e cognome.

Ciò rende Facebook, verosimilmente, la più grande banca dati al mondo di profili pubblici, alimentata dagli stessi utenti identificati direttamente almeno dai dati

---

[295] Cfr ACQUISTI ALESSANDRO, GROSS RALPH AND STUTZMAN FRED, *Face Recognition and Privacy in the Age of Augmented Reality*, Journal of Privacy and Confidentiality, 6(2) (2014)

[296] In argomento per gli indicatori quantitativi si rimanda la capitolo 2 - *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità,* paragrafo 1 - *I dati e le informazioni personali.* Ulteriormente si indica il report leonardo.it - *Tutti i numeri di Facebook: ecco le cifre del social network più famoso del mondo* di Di Ilaria Zanchetta, secondo il quale ogni giorno su Facebook vengono globalmente caricate 300 milioni di foto; ciò rende Facebook probabilmente la più grande banca dati di immagini (in parte pubblica, in parte privata) al mondo.

[297] In proposito si accenna che nell'arco di un decennio tra il 2000 e il 2010 i sistemi di *face recognition* hanno registrato un miglioramento di performance di oltre 3 ordini di grandezza, passando – in condizioni ideali, da un tasso di errore pari a 0,54 ad uno pari a 0,003. Cfr ACQUISTI ALESSANDRO, GROSS RALPH AND STUTZMAN FRED, *Face Recognition and Privacy in the Age of Augmented Reality*, Journal of Privacy and Confidentiality, 6(2) (2014) p.1.

Nome_Cognome_FotoProfilo. Infatti, in generale[298], il profilo social - nei contenuti base di Nome_Cognome_FotoProfilo, è un contenitore pubblico ed accessibile a chiunque: con l'utilizzo congiunto dei software di *face recognizer,* della potenza di calcolo del *cloud computing* e della pervasività dell'*ubiquitous computing,* esso si rivela una base significativa per il successivo arricchimento dei dati con finalità di re-identificazione.

Le sperimentazioni condotte e prese ad esempio hanno previsto: *i)* l'utilizzo un campione di 5000 di foto anonime (prive dell'associazione con i dati identificativi); *ii)* un dominio di 270.000 *primary profile photos* scaricate da Facebook da altrettanti profili (pubblici); *iii)* la comparazione di entrambi gli insiemi mediante il software *PittPatt;*[299] *iv)* l'estrazione del miglior *match score* ad indicatore della positiva (nel senso di statisticamente corretta) corrispondenza di due comparazioni.

A seconda che l'immagine iniziale fosse stata acquisita *on-line* mediante download da repositories pubblici, oppure fornita volontariamente da un utente (ad esempio tramite webcam) le relative sperimentazioni si differenziano, rispettivamente in *on-line re-identifictation* e *off-line re-identification*[300].

Nel primo caso rispetto alle 5000 immagini acquisite on-line, 1 su 10 di esse è stata identificata; nel secondo caso 1 su 3 utenti è stato identificato dopo aver fornito la foto del proprio volto; entrambi i risultati indicano come il dato rappresentativo di un volto anonimo possa essere arricchito con ulteriori attributi descrittivi[301], quindi reso *nonimo* mediante l'utilizzo congiunto di un software di *face redognition* e della base di dati esposta dai *social media.*

Il caso di studio illustrato è una significativa *Proof of Concept* e rappresenta molto bene come dati personali (anche privati) resi volontariamente pubblici dallo stesso soggetto interessato - in uno specifico contesto, per determinate finalità e specifici utilizzi (comunicativi e specificatamente strumentali ai servizi esposti dalla piattaforma social), possano essere riutilizzati in altri contesti, per finalità ed utilizzi diversi ed imprevisti, senza che il soggetto interessato ne sia a conoscenza, quindi impattando in maniera rilevante la protezione dei dati personali con fattive implicazioni di re-identificazione.

---

[298] Questo contesto si riferisce a condizioni di base in cui l'utente in fase di registrazione al social abbia pubblicato una *primary profile photo* contenente il proprio volto e non abbia rilasciato dati identificati falsi

[299] *PittPatt - Pittsburgh Pattern Recognition,* è un software di face recognition sviluppato presso la Carnegie Mellon University (Pittsburgh, Pennsylvania USA) e recentemente acquistato da Google Inc.

[300] Cfr ACQUISTI ALESSANDRO, GROSS RALPH AND STUTZMAN FRED, *Face Recognition and Privacy in the Age of Augmented Reality*, Journal of Privacy and Confidentiality, 6(2) (2014) p. 4; 7.

[301] Nella sperimentazione, volendo porre in risalto la re-identificazione diretta, quindi l'impatto del *data accretion* sulla protezione dei dati personali, l'arricchimento concerne i dati identificativi di nome e cognome senza con ciò limitare qualsiasi altra informazione contenuta nel profilo ed esposta come pubblica.

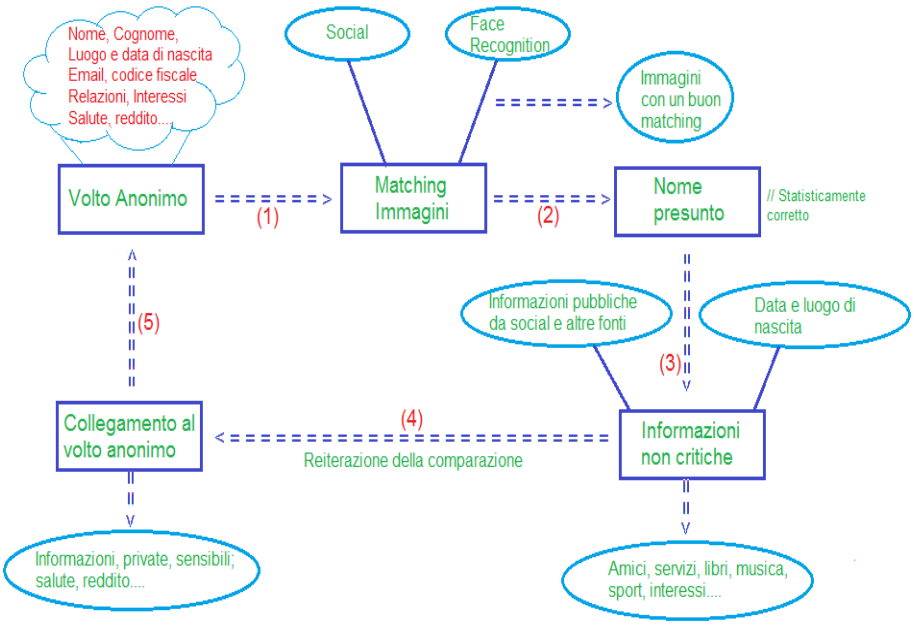


Figura 4.7 – *Data accretion* e re-identificazione.
L'immagine evidenzia il ciclo di re-identificazione: da un volto anonimo - con l'utilizzo di profili social pubblici e un software di *face recognition,* si possano comparare le immagini di migliaia di volti; individuare quello statisticamente corretto, quindi ottenere un nome presunto dal quale ricavare dati personali non privati o non particolarmente sensibili; incrociando queste informazioni con quelle di altre fonti pubbliche, reiterando il processo su molte persone si possono inferire anche informazioni private o sensibili attinenti lo stato di salute, il reddito di uno specifico soggetto; il ciclo si chiude quando il volto anonimo è identificato e il dato che lo rappresenta (immagine) arricchito di ulteriori informazioni e nuovi attributi descrittori.

Oltre ai dati identificativi di nome e cognome, combinando le informazioni degli utenti disponibili sui profili pubblici dei social con altre fonti pubbliche (ad esempio curriculum vitae, informazioni pubbliche della previdenza sociale, della pubblica amministrazione o dell'istruzione) si può implementare concretamente il *data accretion*[302] inferendo informazioni private ed anche sensibili.

[302] Il termine *data accretion* richiama quello dell'incremento del capitale: i dati accrescono se ben combinati insieme, generando nuova informazione così come il capitale accresce se ben investito.
In una prospettiva futura sfruttando la piena affermazione e diffusione dell'*ubiquitous computing* sarà possibile puntare il volto di una persona con uno smartphone, con degli smartglasses o con delle lenti a contatto interconnesse in *cloud;* in tempo reale l'immagine del volto potrà essere arricchita da ulteriori dati, pubblici, personali, privati o sensibili. Allo stato i costi computazionali elevati limitano l'implementazione reale di un simile scenario su larga scala (ad esempio quello rappresentato dalla popolazione di un intero stato con almeno 10 immagini per persona pubblicate sui social), ma tale limitazione tende a diminuire contestualmente al miglioramento degli algoritmi, alla capacità di segmentare il problema in sotto problemi più semplici e parallelizzarne i processi computazionali in *cloud.*

2. LE NUOVE FORME DI VULNERABILITÀ E DI RISCHIO PER LA PROTEZIONE DEI DATI PERSONALI.

Il Regolamento Europeo 679/2016 all'art. 4 *Definizioni,* comma 12) definisce la violazione dei dati personali come *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.*

Questa definizione conferma[303] e rafforza un concetto importantissimo: il problema della violazione dei dati personali non può ritenersi legato (solo) ad azioni intrusive riconducibili al c.d. *hackeraggio,* dirette verso la sfera personale o privata di una persona e poste in essere da attori estranei e *nemici;* alla tradizionale fattispecie dolosa - distinta dalla presenza di un soggetto terzo che volontariamente aggredisce e abbatte il perimetro di protezione posto a presidio delle informazioni personali, si affianca quella accidentale con pari ricadute e danni.

I fattori di *accidentalità* possono essere molteplici e svariati; ma la portata innovativa del GDPR nella direzione della valutazione *ex ante (by default/design)* tanto dell'impatto del trattamento tanto della gravità e della probabilità del rischio per i diritti e le libertà dell'interessato inducono a rintracciare i presupposti delle violazioni – quindi le vulnerabilità e le tipologie di rischio, nelle caratteristiche del trattamento stesso; caratteristiche che risultano configurabili su tre dimensioni: *i)* il dato personale oggetto del trattamento; *ii)* il soggetto identificato o identificabile da tali dati e destinatario del trattamento; *iii)* l'insieme delle operazioni effettuabili sui dati personali che convergono delineandone quindi la natura, il contesto, l'ambito di applicazione e soprattutto la finalità e lo scopo di utilizzo dei dati.

In tutti i contesti informazionali disaminati nei precedenti paragrafi, il soggetto oltre ad essere attore interessato risulta essere soprattutto il principale produttore di informazioni personali trattate (acquisite e dedotte) dalle operazioni di trattamento, rispetto alle quali il mancato mantenimento nel tempo del paradigma *[informativa, finalità e consenso]* concorre a trasformare tale costrutto *da base di liceità a base di vulnerabilità.*

In tal senso l'origine delle criticità, tanto delle misure regolatorie tanto di quelle tecniche di tipo *Privacy-Enhancing Technologies,* risulta rintracciabile:

i. nella generalità dei parametri dell'informativa volta più a favorire l'ambiguità dei contenuti informativi e l'oscuramento delle implicazioni piuttosto che supportare la

[303] Al riguardo si ritiene utile indicare che la definizione trova antecedente sostanziale sovrapposizione nel CODICE italiano all'art. 4 *Definizioni,* comma 3 lettera g-bis) *"violazione di dati personali": violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico.*

flessibilità dei possibili casi d'uso;

ii. nell'eccesso di staticità dei requisiti di qualità del consenso che per quanto robusti in ordine alla specificità, al qualificarsi come informato, libero, incondizionato e inequivocabile rimangono sincronizzati alla sola fase iniziale e di avvio del trattamento e discontinui rispetto allo svolgersi e al differenziarsi dello stesso;

iii. nell'assenza di automatismi applicativi che implementino il mantenimento nel tempo dei requisiti di qualità del consenso rispetto sia alle preferenze dell'utente sia alle caratteristiche dei dati;

iv. nella limitazione di progettare *ex ante* il processo di trattamento in termini delle possibili molteplici finalità e dei dati personali *essenzialmente* necessari al relativo perseguimento.

Rischi e vulnerabilità non possono più essere misurati (solo) *ex post* a violazione avvenuta e a danno fatto, ma devono essere (soprattutto) valutati *ex ante:* previsti e inclusi (unitamente alle contromisure) *by default/design* nella progettazione e nell'avvio stesso del trattamento dei dati personali, connessi tanto alla responsabilità del titolare e del responsabile che il nuovo Regolamento Europeo per la protezione dei dati personali declina in termini di una vera e propria *assunzione di rischio*, tanto all'affermarsi dell'utente come figura centrale che volontariamente *produce, rilascia* e *condivide* informazioni personali, tanto e non ultimo, alle proprietà contestuali (quantitative e qualitative) di tali informazioni comprese quella di essere condivise tra una molteplicità di soggetti.

Nello svolgersi del progetto di ricerca sono state individuate 10 principali tipologie di vulnerabilità e di rischio rispetto alla gestione e quindi alla protezione dei dati personali in contesti di forte inferenza informativa e assimilabili a quelli precedentemente descritti. La scelta che si distingue per uno contributo di novità e di consistenza che supera la classica classificazione delle violazioni[304], rispecchia:

i. la prospettiva innovativa tracciata dal nuovo regolamento europeo sulla scorta dei fondamenti regolatori dalla Direttiva 95/46/CE progressivamente ricalibrati e aggiornati dai pareri del Working Party ex art. 29[305];

[304] In argomento per la tradizionale diversificazione dei rischi e delle violazioni si rimanda al capitolo 2 - *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità,* paragrafo 2.3 *Protezione dei dati personali: le criticità e rischi connessi alla gestione del dato.*

[305] Tra i principali pareri WP ex art.29 che nell'interpretare e direzionare l'applicabilità della Direttiva hanno marcatamente contribuito alla configurazione del nuovo regolamento Europeo si citano:
WP 223, 16 September 2014, *Opinion 8/2014 on the Recent Developments on the Internet of Things* (2014)
WP 216, 10 April 2014, *Opinion 05/2014 on Anonymisation Techniques* (2014)

ii. le limitazioni dell'approccio tradizionale rilevato nella letteratura disaminata, e al contempo la marcata sollecitazione delle contromisure regolatorie proveniente tanto dai principi giuridici quanto dalle applicazioni verso una configurazione della protezione dei dati personali pro-attiva piuttosto che re-attiva orientata ad una tutela del trattamento conforme ai principi di *privacy by design/default*[306]*;* ed in particolare con riferimento al requisito n. 7 del framework *Privacy by Design*[307]

iii. la necessità di prevedere un ruolo centrale e decisore dell'utente nelle fasi di progettazione e avvio garantendone il mantenimento per l'intero ciclo di trattamento; consentire, quindi, alle persone di configurare ed esprimere le loro scelte sulle tipologie e le operazioni di trattamento, per l'intero ciclo di gestione dei propri dati; infine, rimettere nelle mani del soggetto interessato il pieno e continuativo controllo sui dati da questi generati o al quale si riferiscono.

Quest'ultimo punto è stato la direzione portante che ha guidato l'individuazione delle vulnerabilità: ogni qual volta il determinismo informazionale di un artefatto algoritmico (*find engine, data mining, machine learning, corrispondenza semantica*...) - ad esclusivo controllo di un titolare di trattamento, prevale sull'autodeterminazione dell'utente si innesca tra le due parti – e i relativi gradi di responsabilità, una *asimmetria informativa* presupposto e causa delle ulteriori vulnerabilità, dei relativi rischi e delle conseguenti concrete violazioni sui dati personali.

Nei trattamenti *Big Data* la crescente responsabilità degli *artefatti algoritmici* è strettamente connessa ad un determinismo che evolve dall'essere quantitativo al divenire qualitativo e fondato sull'arricchimento semantico dei dati. Nel primo caso ogni risorsa informazionale è sostanzialmente descritta dal numero di visite (o click) conteggiate dall'algoritmo che, con nativa asetticità e in ragione di questa misura ne configura il posizionamento dei collegamenti con le altre risorse.

Nel secondo caso l'*algoritmo* esplica un vero e proprio ruolo di decisore estraendo e analizzando gli attributi portati da ciascun dato, la loro semantica, discriminandone la rilevanza

WP 221, 16 September 2014, S*tatement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU* (2014)
WP 202, 27 February 2013, *Opinion 02/2013 on apps on smart devices* (2013)
WP 187, 13 July 2011, *Opinion 15/2011 on the definition of consent* (2011)
WP 163, 12 June 2009, *Opinion 5/2009 on online social networking* (2009)
WP 148, 4 April 2008, *Opinion 1/2008 on data protection issues related to search engines* (2008)
WP 136, 20 June 2007, *Opinion 4/2007 on the concept of personal data* (2007)

306 Per un maggior approfondimento sui requisiti e le best practices del framework *Privacy by Design/Default* si rimanda al capitolo 3 - *Privacy e Protezione dei Dati personali: le contromisure*, paragrafi 3 *La protezione dei dati personali come requisito intrinseco di processi e servizi* e 3.1 *Il framework Privacy by Design e Privacy by Default.*

307 Esso attiene la centralità dell'utente (*Respect for User Privacy – Keep it User-Centric*)

del contenuto non tramite conteggi ma tramite correlazioni e attinenze semantiche; arricchisce, classifica, deduce nuovi descrittori, predice e relaziona le informazioni; e sugli esiti di tutte queste operazioni confeziona servizi personalizzati all'utente quando i dati trattati concernono e identificano direttamente o indirettamente le persone. Questo flusso di *data accretion*[308] tende, non secondariamente, a minimizzare l'interazione con l'utente sfruttando al massimo i dati personali inizialmente condivisi e rilasciati, operando (al contempo) in maniera quasi silenziosa e invisibile.

La matrice di criticità comune alle tipologie di vulnerabilità disaminate si attua quando al crescere della responsabilità del determinismo informazionale algoritmico corrisponde una pari o maggiore deresponsabilizzazione (al limite esclusione) dell'utente; e la silenziosità algoritmica limita o compromette la trasparenza verso l'utente; quando sulla verifica del dato prevale la sua quantità, il moltiplicarsi incontrollato, il riutilizzo diversificato. Da ciò discende una conseguente perdita di controllo sulle proprie informazioni personali, dispersione che a sua volta ciclicamente accresce l'asimmetria informativa.

La ricaduta tangibile di questo flusso è la degenerazione di una personalizzazione volta ai benefici e ai vantaggi, in una personalizzazione percepita dagli utenti con negatività, fastidio, sfiducia, al limite anche come invasività e pericolo e, spesso, opposta con l'abbandono o la rinuncia all'utilizzo dei servizi o peggio l'immissione in rete di dati distorti, falsi (c.d. fake), inutili e di scarsa qualità; ciò con intuibili ricadute per la *veracità* e il *valore* della relazione tra dati, quindi l'affidabilità e lo sviluppo del sistema nel suo complesso.

La figura che segue sintetizza e collega graficamente i 10 principali contesti di vulnerabilità descritti nel proseguo del paragrafo. In chiusura, dopo la descrizione delle 10 vulnerabilità, viene prodotta una tabella che relaziona queste nuove tipologie con i relativi rischi e il conseguente aggiornato spettro di violazioni della *privacy* e dei dati personali, all'interno del quale trovano naturale ricollocazione anche quelle tradizionali concernenti la violazione dell'anonimato e la re-identificazione di dati anonimi, il furto di identità e l'impersonazione, il furto e l'utilizzo illecito di informazioni personali.

[308] Cfr precedente paragrafo 1.3 - *Realtà aumentata e Data Accretion*

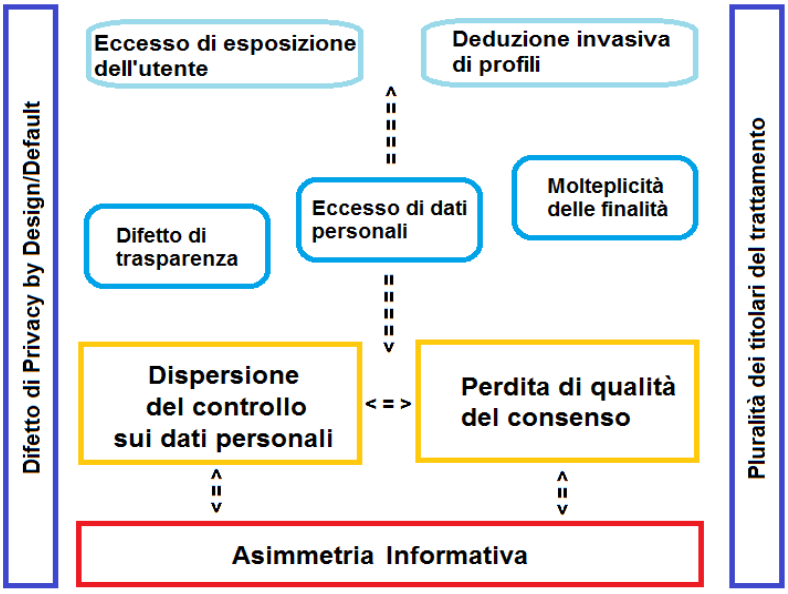


Figura 4.8 – Nuovo scenario di vulnerabilità e di rischi per la protezione dei dati personali.
I nuovi scenari di vulnerabilità comprendono: l'asimmetria informativa tra chi produce le informazioni e chi le sfrutta; il mantenimento degli indicatori di qualità del consenso nel suo configurarsi *informato, libero, specifico, inequivocabile e concludente;* la dispersione e la perdita di controllo sulle dati personali; l'eccesso di dati personali (ridondanza e massimizzazione quantitativa nell'utilizzo dei dati personali); la molteplicità e il proliferare finalità di utilizzo incontrollate; il difetto di trasparenza; l'eccesso di esposizione del soggetto interessato, la deduzione invasiva di attitudini e aspetti della personalità; oltre a vulnerabilità collegabili alla pluralità dei titolari componenti la filiera degli stakeholders e alla scarsa nativa compliance *privacy by design/default* dei trattamenti.

Risulta non pleonastico precisare che questa classificazione riguarda una possibile categorizzazione delle vulnerabilità e dei rischi specificatamente attinenti la gestione delle informazioni personali, quindi la *privacy* e la protezione dei dati personali e non la sicurezza delle informazioni (anche personali), spettro in cui vengono ricompresi prioritariamente i tipici attacchi alla sicurezza e volti contro la confidenzialità, l'integrità e la disponibilità delle informazioni[309,310].

[309] Gli attacchi alla confidenzialità comprendono le seguenti categorie: intercettazione di pacchetti, reupero di parole chiavi, scansione delle porte, interrogazione con PING, *dumpster diving, keylogger, phishing, pharming,* l'ingegneria sociale.
Gli attacchi all'integrità comprendono le seguenti categorie: salami attacks, data diddling, man-in-the-middle, session hijacking.
Gli attacchi alla disponiblità comprendono le seguenti categorie: Denial of Service, Distributed Denial of Service, Flood.
Cfr D'Acquisto G., Naldi M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017) p. 191 – 201.

[310] Solo per citare il più recente attacco in ordine di accadimento, *WannaCry 2.0* è un virus ransomware che - sfruttando un difetto di aggiornamento in sistemi operativi Windows, il 12 Maggio 2017 ha causato una vera e propria epidemia digitale cifrando su larga scala dati memorizzati in sistemi informatici di aziende e organizzazioni di tutto il mondo allo scopo di chiedere un riscatto pari a 300 dollari in bitcoins per decriptarli. Questo esempio rappresenta una tipica azione dolosa di cybercrime contro la sicurezza delle informazioni e non tanto contro la privacy, non sussistendo determinazioni di re-identificazione, impersonazione o furto di dati identificativi, ma *semplicemente* quella volta al ricatto per il ripristino delle informazioni. Cfr https://it.wikipedia.org/wiki/WannaCry

2.1. ASIMMETRIA INFORMATIVA. DISPERSIONE DEL CONTROLLO SUI DATI PERSONALI. PERDITA DI QUALITÀ DEL CONSENSO.

ASIMMETRIA INFORMATIVA.

L'asimmetria informativa è un concetto molto applicato in economia e in teoria dei giochi, attiene lo scenario in cui tra due controparti (due giocatori, azienda-cliente) ricorre uno sbilanciamento di informazione rispetto ad una data decisione, ad un dato fenomeno e ai relativi comportamenti. Chi dispone di maggiori e migliori informazioni esercita un vantaggio sull'altra parte che implicitamente subisce uno svantaggio. Questo sbilanciamento si misura in termini di esternalità (positiva per il destinatario dei vantaggi, negativa per la controparte), con implicazioni di *selezione avversa*[311] e *azzardo morale*[312] e può essere riequilibrato con una sorta di somministrazione di informazione - l'*informazione derivata,* che la parte meno informata può utilizzare per compensare l'originaria carenza. Ulteriore caratteristica e conseguenza dell'asimmetria informativa è quella della *razionalità limitata.*

La presenza di informazione carente o incompleta influisce sul processo decisionale di utilizzo dei propri dati e, quindi, sulla loro protezione; utilizzi e violazioni possono essere scoperte solo a posteriori, dopo aver messo a confronto dati o eventi futuri. La *razionalità limitata* concerne l'incapacità di prevedere, misurare e confrontare le implicazioni di rilascio e di uso delle proprie informazioni, nonché i fattori di rischio e gli elementi di vantaggio.

In un contesto di gestione dei dati personali in cui le controparti economiche possono trovare corrispondenza nel soggetto interessato e nel titolare del trattamento algoritmico, le caratteristiche sopra indicate possono essere relazionate con le vulnerabilità e i rischi connessi alla protezione delle informazioni, cosicché da configurare l'asimmetria informativa come principale presupposto e implicazione di criticità per la *privacy.*

In tale contesto il titolare del trattamento algoritmico è la parte più informata potendo sfruttare sia una originaria ridondanza di dati che l'esclusiva prerogativa di elaborarne e ampliarne il significato con mezzi e risorse di gran lunga superiori a quelle disponibili al

[311] La selezione avversa è un problema connaturato al divario tra le informazioni possedute dall'azienda e quelle possedute dal cliente. Studiata inizialmente da Akerlof negli anni settanta, oggi trova applicazione soprattutto nel mercato assicurativo o bancario. In quest ambiti la maggiore informazione (di cui l'assicurazione o la banca non dispone) consente al cliente una più conveniente operazione di stipula.
Cfr https://it.wikipedia.org/wiki/Asimmetria_informativa

[312] L'azzardo morale è una forma di opportunismo post-contrattuale che si verifica durante il rapporto assicurativo. Il consumatore, avendo stipulato un contratto che lo tutela e lo risarcisce in caso di accadimento dell'evento negativo, è portato a non usare più strumenti e accortezze cautelari che lo prevengano dall'evento. Il fatto di essere assicurato induce l'individuo a ridurre l'attività di prevenzione o parallelamente a sovrautilizzare la disponibilità di risorse a lui dovute più di quanto non necessiti.
Cfr https://it.wikipedia.org/wiki/Asimmetria_informativa

soggetto interessato, il quale in scenari informazionali *data intensive* e di trattamento basato sullo s*chema Big data* spesso non si accorge nemmeno di questa prevalenza informativa del titolare; questi può assumere decisioni di cui le persone non sono consapevoli, oppure *clusterizzare* le deduzioni ignorandone le diverse valenze semantiche al variare dei soggetti interessati.

Inoltre l'alterazione dell'asimmetria informativa si rivela difficilmente ripristinabile per l'assenza o l'inadeguatezza delle risorse, oppure per l'inefficacia delle misure nel caso limite di fatti (riservati) divenuti di dominio pubblico e privi di filtri, sui quali è impensabile pretenderne la totale cancellazione dai sistemi informativi e dalla memoria delle persone.

DISPERSIONE DEL CONTROLLO SUI DATI.

L'interpretazione della protezione dei dati personali come controllo degli stessi rende possibile interpretare l'asimmetria informativa come una dicotomia di *privacy:* la prima forma implica che il soggetto interessato conosce informazioni sul proprio conto ad altre parti indisponibili; la seconda forma invece si presenta quando il soggetto perde il controllo sui propri dati.

In contesti di asimmetria informativa il soggetto dopo aver fornito ad altre parti informazioni personali perde il controllo sulle stesse per intervalli di tempo imprevedibili, senza poter conoscere come, quando, chi e per quali ragioni saranno utilizzate. La persona che rilascia i dati (con o senza consenso) attiva, a sua volta, una ulteriore posizione di asimmetria informativa per ciò che attiene l'ulteriore e secondario utilizzo, la disseminazione degli stessi da parte di altri soggetti.

I flussi di informazioni creati dal trattamento *Big Data* e connessi alla relazione tra diversi dati e tra dati ed oggetti, difficilmente possono essere gestiti ricorrendo ai classici strumenti utilizzati per garantire una tutela adeguata delle libertà e dei diritti dell'interessato. Ancor prima di poter azionare i propri diritti di controllo il soggetto interessato difficilmente è posto nelle condizioni di essere partecipe e di poter riesaminare gli esiti di processamento tra i dati grezzi e aggregati, prima che ne avvenga la loro pubblicazione.

La perdita di controllo sui propri dati è molto evidente negli scenari *IoT* in quanto rilevabile sin dalla fase iniziale della raccolta. In tali sistemi la comunicazione tra gli oggetti (ciò che in uno schema *Big Data* diventa la relazione tra dati) può essere avviata automaticamente e tramite impostazioni predefinite, senza che il diretto interessato ne sia al corrente.

L'impossibilità di controllare efficacemente l'interazione o di stabilirne il dominio virtuale rende estremamente difficile monitorare il flusso di dati generato, così come i successivi e diversi utilizzi e la diversificazione delle finalità.

PERDITA DI QUALITÀ DEL CONSENSO.

Questa vulnerabilità attiene il mancato mantenimento nel tempo dei requisiti di qualità del consenso, ovvero il mantenersi: libero, informato, specifico ed inequivocabile. In particolare il secondo e il terzo requisito rilevano la carenza di chiarezza e di dinamicità del meccanismo del consenso nell'adattarsi e nel riformularsi al variare del trattamento dei dati personali ogni qual volta agli scopi e agli utilizzi principali se ne affiancano di ulteriori distinti per tipologia di dati utilizzati, mezzi, ambito di applicazione e destinatari del trattamento.

In molti casi, il soggetto interessato è totalmente inconsapevole tanto del trattamento dei dati effettuato da *smart devices* (del tutto indistinguibili dai corrispondenti oggetti non connessi) tanto da quello effettuato da artefatti algoritmici di *find engine* o *data mining* il cui successo della personalizzazione dipende da quanto più invisibili sono il processamento e la relazione dei dati e da quanto meno coinvolto risulta essere l'utente.

L'impossibilità di identificare il trattamento ed di intervenire su di esso - ad esempio ogni qual volta sensori registrano e trasferiscono dati oppure titolari del trattamento si scambiano informazioni per ampliarne gli attributi descrittivi e quindi arricchire i fenomeni rappresentati, configura un consenso di *bassa qualità* fondato su una mancanza di informazione o sull'impossibilità di fatto a renderlo ben calibrato e tale da tener conto delle preferenze espresse dal soggetto interessato; il quale – non secondariamente, spesso si trova ad agire in due possibili situazioni nel rilasciare l'autorizzazione al trattamento: *i)* quella in cui è condizionato dall'assenza di alternative o eccezioni se non quella di rinunciare al servizio associato al trattamento; *ii)* e quella in cui è fuorviato da un'eccessiva generalità descrittiva e da informazioni ambigue o poco comprensibili. Entrambi i casi configurano un consenso non libero.

L'inefficacia del consenso rende lo stesso non utilizzabile come base giuridica di trattamento, che in assenza di alternative condizioni di liceità (cfr art. 6 GDPR - *Liceità del trattamento*) risulta anch'esso privo di efficacia giuridica.

2.2. Difetto di trasparenza. Eccesso di dati personali. Molteplicità delle finalità.

Difetto di Trasparenza.

I trattamenti posti in essere in ambiti applicativi *data intensive* si distinguono dall'essere tanto più efficienti quanto più invisibili e privi di sistemi di notifica. Oggetti *IoT* e *app* installate su smartphone raccolgono e scambiano dati in modalità discreta, continua, pervasiva - senza il più possibile ricorrere all'intervento o alla partecipazione dell'utente interessato. Analogamente motori di *find engine* mascherano i passaggi intermedi tra la richiesta e il risultato connessi all'arricchimento dei dati, all'indicizzazione, al collegamento e alla classificazione.

A questo eccesso di invisibilità corrisponde un difetto di trasparenza che alimenta l'asimmetria informativa e che preclude il principio di lealtà con cui dovrebbero essere trattati i dati personali - i quali non dovrebbero mai essere raccolti ed elaborati senza che il soggetto interessato ne sia informato e consapevole; principio che, tra l'altro, rappresenta condizione necessaria e sufficiente affinché e a prescindere dal rilascio del consenso, la persona interessata possa azionare e mantenere i diritti di controllo sull'intero ciclo di trattamento.

Eccesso di dati personali.

Questa vulnerabilità si configura quando l'implementazione di un trattamento raccoglie e conserva tipologie e quantità di dati superiori al minimo richiesto per lo specifico utilizzo o la prefissata finalità. L'analisi di questa criticità, che comporta indubbie implicazioni di perdita di controllo sui dati e di asimmetria informativa, dipende fortemente dall'ambito applicativo e dal contesto del trattamento e richiede necessariamente un contemperamento di più fattori. Ad esempio una limitazione sul numero dei dati risulterebbe contraddittorio in uno *schema Big data* dove dalla ricchezza e dalla diversificazione degli attributi descrittivi discende l'accuratezza e la veracità delle deduzioni; per altro verso un eccesso di informazioni scarsamente pertinenti implicherebbe conseguenze inverse con deduzioni false e ingannevoli.

Il concetto di base quindi non è assoluto ma deve essere rapportato alla finalità; l'utilizzo eccessivo di dati personali sicuramente ricorre quando vengono raccolti per scopi futuri o probabili utilizzi: l'approccio "*intanto richiedo un certo dato all'utente, e se necessario poi lo utilizzo*" si rivela non solo una complicazione di gestione: tecnica – se del dato, ad esempio, di deve provare la provenienza o analizzarne l'aggiornamento; giuridica – atteso che un'informazione

così raccolta non può essere presupposto di un consenso specifico; ma soprattutto si rivela un fattore di rischio di esposizione dell'utente a profilazione invasiva basata su un dato non essenziale comunque nella disponibilità del titolare.

Altra forma di massimizzazione dei dati personali può essere rintracciata nella condivisione e nella mancata cancellazione di dati grezzi, essendo invece necessari - per lo specifico scopo, dati in forma aggregata.

Inoltre il concetto di utilizzo eccessivo di dati personali attiene non solo l'informazione in quanto tale ma anche l'utilizzo o l'attivazione di servizi non necessari (eccessivi) se non inutili in un determinato contesto[313].

Infine, la massimizzazione dei dati personali incide non residualmente sul processo di anonimizzazione - se considerato forma limite di sottrazione e minimizzazione dei dati identificativi, favorendo la re-identificazione del soggetto interessato.

MOLTEPLICITÀ DELLE FINALITÀ.

Questa vulnerabilità attiene l'incapacità di mantenere nel tempo la finalità originaria di un trattamento o di associarne una compatibile; è un problema intrinseco di tutti gli ambiti informazionali *data intensive,* distinti da scambi di dati voluminosi, pervasivi e continui nel tempo.

Il trattamento di dati basato su schema *Big Data* avente come dominio l'*IoT* o le *Apps* per *smart devices,* implementato con tecniche di analisi predittive, aggregazione e di controllo incrociato può nativamente portare a utilizzi secondari di questi dati, relativi o meno allo scopo assegnato al trattamento originario. Dati originariamente raccolti attraverso un dispositivo (ad esempio il giroscopio di uno *smartphone* o il *cookie* di un browser) possono quindi essere utilizzati per ottenere altre informazioni con un significato completamente diverso (ad esempio le abitudini di guida o della navigazione internet della persona).

Ogni soggetto terzo che accede a dati precedentemente ampliati da altri titolari potrebbe ri-utilizzarli per scopi diversi e totalmente incontrollati per l'assenza di un consenso specifico.

---

313 I dispositivi *IoT* sono progettati per essere direttamente accessibili via Internet, non sono solitamente configurati dall'utente e funzionano in modalità di default. Possono, quindi, rivelarsi una facile via d'accesso per intromissioni e tipici attacchi alla sicurezza contro la confidenzialità, l'integrità e la disponibilità. alla confidenzialità che potrebbero essere evitati disabilitando by default funzioni di rete non necessarie.
Cfr il parere Working Party ex art. 29 n. 223, 16 September 2014, Opinion 8/2014 *on the Recent Developments on the Internet of Things. (*p. 21 IT)

2.3. Eccesso di esposizione dell'utente. Deduzione Invasiva di Profili.

Eccesso di esposizione dell'utente.

La ridondanza e l'eccesso di dati personali implicano la crescita di dettagli e dei relativi attributi descrittivi che non sempre si rivelano un veicolo di inferenze di qualità, quindi efficaci e utili per una personalizzazione positiva. In ogni caso il trattamento effettuato da algoritmi o da oggetti lascia scarso margine di convalida per il soggetto interessato, il quale raramente è in grado di intervenire e riesaminare gli esiti del processamento che trasforma i dati dal formato grezzo, a quello strutturato e a quello aggregato rappresentativo di deduzioni e nuova informazione.

Dalla condivisione di informazione priva di schermo ed eccessivamente dettagliata possono emergere conseguenze non solo in ordine alla conoscenza (quantitativa) di dati che il soggetto interessato ignora possano essere nella disponibilità altrui ma anche in ordine alla loro corretta semantica: titolari e diversi soggetti destinatari conoscono non solo troppa informazione ma anche di scarsa veridicità, sorgenti informative di false o distorte verità o di alterazione dei fatti della vita difficilmente ripristinabili se divenuti di dominio pubblico.

Deduzione invasiva di profili.

Il volume di dati raccolti e analizzati può rivelare aspetti specifici delle abitudini, dei comportamenti e delle preferenze del soggetto interessato favorendo importanti capacità di profilazione, di rilevazione di modelli di comportamento e di vita molto dettagliati e completi.

Da ciò derivano due implicazioni: l'impatto sul modo in cui una persona si comporta in risposta alla percezione di essere soggetta ad una sorveglianza molto pervasiva per la propria intimità e la propria vita privata, e quindi sollecitata a comportamenti non spontanei potenzialmente interpretabili come anomalie; la seconda attiene la catalogazione del soggetto interessato in profili con determinate caratteristiche e rispondente a determinati canoni, tali da implicare la degenerazione della differenziazione di servizi in discriminazione attuata, per esempio, con la negazione di accesso ad un bene o a servizio; l'associazione di un prezzo in relazione al proprio stato senza poter esercitare alcuna negoziazione; o ancora l'omologazione dei gusti per l'appartenenza ad un determinato profilo con preclusione di nuove alternative rispetto alla scelta di contenuti direzionati su quelli ritenuti più vicini e affini alla propria personalità e alle proprie attitudini.

2.4. DIFETTO DI PRIVACY BY DESIGN/DEFAULT. PLURALITÀ DEI TITOLARI DI TRATTAMENTO.

DIFETTO DI PRIVACY BY DESIGN/DEFAULT.

Il presidio delle informazioni personali tende ad essere prevalentemente configurato con un approccio e una valenza sostanzialmente difensiva, re-attiva; ciò porta a concentrare le contromisure su attacchi e violazioni oltre che aleatori, difficilmente rimediabili a violazione avvenuta. Questo approccio si rivela inadeguato in contesti *data intensive* in cui l'abbondanza dei dati e la contingente necessità di un accrescimento e di un ri-utilizzo delle informazioni, interoperabile e condiviso tra molteplici soggetti, rendono per un verso inutile la perimetrazione degli utilizzi e degli utilizzatori per un altro non più possibile la restrizione dei confini di trattamento ad uno solo ambito al fine di ridurre i casi di utilizzo illecito.

La carenza di *privacy by default* si attua non nell'incapacità di contrastare gli attacchi, ma nel rendere gli stessi dati meno affidabili e meno sicuri o perché trattati nell'ambito di processi de-strutturati, parcellizzati e mal-pensati in origine o perché elaborati da oggetti che non incorporano nativamente componenti di *anonimizzazione* e *pseudoanonimizzazione.*

La carenza di *privacy by design* si attua non nell'esporre il dato ad attacchi esterni bensì ad un degrado di qualità oltre che ad un eccesso quantitativo di dati personali.

Non secondariamente un difetto di *privacy by design* implica immediatamente una incompletezza del quadro progettuale di definizione del trattamento contestuale alla raccolta delle informazioni; ciò impedisce la completa determinazione del dominio dei dati e delle finalità prima che abbia luogo il trattamento, esponendo lo stesso a cambiamenti e adattamenti improvvisi. Inoltre, tanto i trattamenti attuati nell'*IoT* quanto quelli con schema *Big Data* non sono progettati per fornire autonomamente e *by default* informazioni sull'evolversi del trattamento in termini di tipologie di dati trattati, utilizzi e finalità secondarie, rivelandosi quindi incapaci di implementare dinamicamente una nativa rimodulazione del consenso da riformulare e riproporre al soggetto interessato.

PLURALITÀ DEI TITOLARI DI TRATTAMENTO.

Gli attori coinvolti in uno schema di trattamento *Big Data,* specie se basato sulla raccolta e l'elaborazione di informazioni dell'*IoT* o delle *APPs* configurano una complessa ed

eterogenea rete di portatori di interesse tutti connotabili come titolari/responsabili del trattamento nella misura in cui ne definiscono mezzi e finalità, gestiscono regole e algoritmi di processamento.

La criticità attiene tanto la ripartizione e l'interconnessione dei rispettivi compiti applicativi - fattore che limita o comunque complica una effettiva interoperabilità dei sistemi e delle applicazioni, così come la standardizzazione e la portabilità dei dati; tanto la ripartizione delle responsabilità giuridiche in ordine agli obblighi di trasparenza, di acquisizione del consenso, della condivisione e della propagazione delle decisioni del soggetto interessato in esito ai diritti di controllo azionabili: quindi una decisione di revoca del consenso, di limitazione e opposizione al trattamento o ancora la richiesta di cancellazione di dati personali difficilmente trova una congiunta convalida e applicazione tra tutti i titolari coinvolti.

Non secondariamente la compresenza di molteplici titolari può implicare violazioni della sicurezza del sistema nel suo complesso mediante attacchi alla confidenzialità, all'integrità e alla disponibilità.

Vulnerabilità / Rischi	**Difetto di trasparenza**	**Eccesso di dati personali**	**Molteplicità delle finalità**
Asimmetria informativa	**Eccesso di esposizione dell'utente** Impossibilità di riesaminare l'informazione	**Eccesso esposizione dell'utente** Eccesso di personalizzazione Perdita anonimato	Violazione confidenzialità Violazione integrità
Dispersione del controllo sui dati personali	**Eccesso esposizione dell'utente** Perdita anonimato Impersonazione	**Eccesso di esposizione dell'utente** False verità Distosione fatti della vita Mantenimento pubblico di fatti riservati	**Deduzione invasiva di profili** Clusterizzazione di profili Omologazione delle preferenze
Perdita della qualità del consenso	**Eccesso di esposizione dell'utente** Impossibilità di riesaminare l'informazione	Violazione confidenzialità Violazione integrità	**Deduzione invasiva di profili** Discriminzione Accesso negto a beni o servizi (utente fuori canoni) Impossibilità a negoziare il prezzo di un bene.

Tabella 4.1 - Le nuove forme di vulnerabilità e di rischio per la protezione dei dati personali.

3. LA GARANZIA DI QUALITÀ DEI DATI E LE NUOVE TIPOLOGIE DI RISCHIO PER LA *PRIVACY.*

Vulnerabilità, rischi e violazioni possono essere configurati in termini di quantità e qualità dei dati; se la questione venisse attenzionata dallo speculare punto di vista delle contromisure e ci si ponesse la domanda: *una gestione del dato (personale) più efficiente (con attinenza, quindi, al contenimento della quantità delle informazioni) e più efficace (con attinenza, quindi alla qualità e alla caratteristiche dei dati) potrebbe prevenire o contenere i rischi elencati, o comunque ridurne probabilità e gravità?* La risposta si rivelerebbe affermativa per ognuna delle tipologie di vulnerabilità trattate, la cui radice comune può essere rintracciata tanto nell'interruzione della qualità del dato e tanto dell'efficacia della sua gestione.

La qualità dei dati è strumentale per comprovarne la validità della gestione e del processamento. Lo standard UNI ISO/IEC 25012 (2008) fornisce un modello di descrizione e rilevazione della qualità delle informazioni basato sulla presenza e la valorizzazione di alcuni campi (proprietà e attributi), volte a evidenziarne tanto la conformità rispetto alla tipologia e alle caratteristiche di gestione (quindi rispetto dell'insieme di applicazioni, dei vincoli regolatori, e dei controlli dell'attività di processamento), tanto la corrispondenza al fenomeno rappresentato.

Il modello suddivide in due gruppi le proprietà che un dato dovrebbe avere per essere considerato di qualità nonché per innescare e configurare una pari gestione (quindi un trattamento di qualità).

Nel primo gruppo rientrano caratteristiche intrinseche al dato: l'*accuratezza*, *correttezza* o *esattezza* – indicatore volto a misurare la rispondenza del dato al fenomeno rappresentato; l'*attualità* – indicatore di contingente aggiornamento; la *coerenza* – indicatore di non contraddittorietà tra gli gli attributi dello stesso dato o descrittivi di altri dati; la *completezza* e l'*essenzialità* – volte a misurare rispettivamente la presenza di un numero sufficiente o necessario di informazioni per rappresentare il contesto descritto; la *credibilità* – ad indicazione della provenienza da fonte certa.

Nel secondo gruppo rientrano le caratteristiche attinenti o dipendenti dai sistemi di gestione: l'*accessibilità* – ovvero la garanzia di accesso anche in condizioni di criticità*;* la *comprensibilità* – indicatore di chiarezza, immediatezza e non ambiguità; la *conformità* – quale indicatore del rispetto di specifiche regolamentazioni e scopi d'uso; l'*efficienza* – a misura di un utilizzo con risorse e tempi adeguati allo scopo; la *precisione* – attinente l'adeguatezza del sistema di misura; la *disponibilità, l'interoperabilità* e la *portabilità* – attinenti la possibilità di

interrogare e migrare il dati tra diversi sistemi di processamento; la *riservatezza,* la *tracciabilità* e la *recoverabilità* – ad indicazione che il dato è conservato in un ambiente sicuro, tracciato nell'accesso, riservato agli utenti autorizzati.

Il decremento o la perdita di qualità portano un costo in termini di inefficienze, limitazioni, ritardi o al limite preclusione e diniego all'accesso e alla fruizione di un determinato servizio; il rischio rappresentata il valore massimo di questo costo.

La probabilità e la gravità di questo rischio sono intrinsecamente connesse al prevalere della quantità dei dati (quindi del loro uso e ri-uso), sulla qualità, sulla verifica e sul mantenimento nel tempo dei requisiti e degli indicatori elencati. I contesti informazionali *data intensive* risultano nativamente a rischio rispetto alle vulnerabilità di *privacy* e di protezione dei dati personali non solo per la circolazione in chiaro tipica delle reti pubbliche, ma per la crescente disponibilità di volumi di dati.

Le misure di protezione delle informazioni personali vanno pensate come una sorta di ingegnerizzazione della qualità dei dati volta ad automatizzarne l'inserimento *by default,* il mantenimento e la verifica continua dei requisiti e degli indicatori. La garanzia di qualità dei dati diventa lo strumento per adempiere all'obbligo posto in capo ai titolari di integrare nel trattamento il requisito di tutela dei diritti e delle libertà dei soggetti interessati, di implementare il paradigma portante rappresentato da *[informativa, finalità, consenso]* nonché consentire agli interessati l'esercizio dei diritti azionabili per il controllo delle proprie informazioni[314].

Su quest'ultimo punto, in particolare, i nuovi diritti introdotti dal GDPR – diritto alla portabilità e diritto all'oblio possono essere interpretati come comprova di qualità del dato: il primo scoraggiando inaccuratezza e obsolescenza rispecchia e favorisce esattezza, pertinenza, attualità e interoperabilità; il secondo – se lo si considera nella funzione base di de-indicizzazione dei collegamenti posizionati da un motore di ricerca, favorisce la minimizzazione dell'utilizzo del dato richiedendo l'eliminazione di quelli ritenuti inutili superati e non più validi dall'utente.

La qualità del dato verso la finalità del trattamento. I requisiti di qualità non sono concetti astratti o assoluti ma devono essere rapportati alle caratteristiche del fenomeno rappresentato dagli stessi dati e quindi alla loro finalità d'uso; il trattamento di informazioni digitali che

[314] Cfr D'Acquisto G., Naldi M., Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza, G. Giappichelli Editore (2017) p. 174-177.

implicano una ricaduta diretta e misurabile sulla persona non possono prescindere dal processare dati di accertata qualità sia in ordine all'*esattezza,* sia in ordine al mantenimento della *coerenza* tra i dati rilasciati dal soggetto interessato e quelli ricavati dal processamento algoritmico, tra i quali non dovrebbero sorgere collisioni o contraddizioni. La non compromissione del conseguimento della finalità passa anche per la qualità della descrizione semantica del dato rispetto ai requisiti di *chiarezza, immediatezza* e *interoperabilità.*

Questo aspetto risulta essenziale nei casi in cui più titolari decidono di condividere il rispettivo dominio per concorrere al perseguimento di una medesima e prefissata finalità: l'adozione di formati sintattici e semantici comuni nella descrizione degli attributi dei dati non è solo un fattore necessario per incrociarne le relazioni ma si rivela essenziale per garantirne pertinenza e rilevanza minimizzando i costi di interconnessione e il rischio di diversificare o non perseguire gli scopi di utilizzo[315].

La qualità del dato verso la responsabilità del trattamento. La distinzione dei requisiti di qualità in due gruppi, supporta (in particolare nei casi di trattamenti complessi) una migliore ripartizione delle responsabilità connesse al trattamento separando quelle relative alla raccolta dei dati - per le quali è importante verificare i requisiti di qualità nativi al dato (primo gruppo), da quelle connesse alle successive elaborazioni per le quali gli indicatori di qualità dipendono anche dai sistemi e dalle applicazioni di trattamento (secondo gruppo).

Inoltre, e non secondariamente, la misura *ex ante* della qualità delle informazioni sottoposte a trattamento concorre nel definire non solo <...*le misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento....*>[316], ma anche a misurare e differenziare le responsabilità (ed eventualmente le sanzioni) tra i vari contitolari[317] qualora la violazione riguardasse informazioni in origine inesatte, non attuali, eccessive o non pertinenti.

La qualità del dato verso la portabilità (e viceversa). L'interoperabilità del dato è *conditio sine qua non* per la *portabilità;* la quale a sua volta alimenta il circolo virtuoso verso l'*esattezza* e la *pertinenza* ponendo il vincolo pratico (ovvero lo scambio verso il soggetto o verso altri titolari) di evitare ogni sconveniente e penalizzante forma di inaccuratezza.

---

315 In merito, un esempio può essere rintracciato nel caso in cui un vettore di trasporti aerei o ferroviari e una catena di hotels siano disponibili ad un accordo commerciale finalizzato all'erogazione di servizi di viaggio arricchiti da offerte di soggiorno. La condivisione e l'incrocio dei rispettivi domini di dati è un elemento necessario al successo dell'iniziativa a condizione che le sfere di influenza dei dati e la descrizione degli attributi siano espressi nello stesso formato, veicolati dallo stesso linguaggio e prevedano gli stessi costrutti semantici.

316 cfr GDPR, Articolo 24 *Responsabilità del titolare del trattamento*

317 cfr GDPR, Articolo 26 *Contitolari del trattamento*

La qualità del dato verso la trasparenza e il consenso. Gli indicatori di *credibilità, accessibilità comprensibilità, precisione* si rivelano fondamentali per la valutazione delle fonti di provenienza del dato, l'adeguatezza dei sistemi di misura, l'efficacia e la semplicità della rappresentazione, come tali volti a ridurre arbitrarietà e ambiguità sia verso l'esposizione dell'informativa all'utente sia verso l'interpretazione algoritmica, spesso distinta da criteri *oscuri* difficilmente accessibili e valutabili.

L'affidabilità qualitativa dei dati - veicolata in particolare dagli indicatori di *esattezza*, *completezza* ed *essenzialità,* è necessario sia garantita soprattutto in fase di raccolta e rilascio iniziale delle informazioni acconsentite dal soggetto interessato: pensare l'avvio del trattamento su dati qualitativamente robusti perché esatti, completi/non ridondanti, non contraddittori favorisce e supporta la qualità del consenso associato al rilascio in ordine, soprattutto, all'essere informato nell'esposizione ed inequivocabile nel riscontro.

Inoltre, e non secondariamente, porre in qualità la fase di *disclosure* delle informazioni minimizza il rischio di eccesso e massimizzazione dei dati personali nonché della contestuale ed immediata implicazione di asimmetria informativa.

Questa questione si rivela significativa, evidente e soprattutto misurabile non solo in contesti di *data intesive* e trattamento *Big Data* già a pieno configurati nella loro voluminosità e varietà; bensì anche nella *contenuta* e *circoscritta* fase di rilascio di dati personali per esempio nel trattamento di registrazione ad un servizio on-line, durante il quale risulta importantissimo rilasciare il minimo numero di dati coerenti e pertinenti allo scopo e all'utilizzo, al fine di evitare rilascio e moltiplicazione di dati inutili quando di incerto controllo da parte dell'utente.

Su questo aspetto nel capitolo 5 – *Progettazione di un modello di supporto a politiche di privacy user e data centric,* paragrafo 1 – *L'applicazione delle Privacy Policies di tipo User-centric,* viene illustrata una *Proof of Concept* che evidenzia la presenza del rischio di *eccesso di dati personali* nella registrazione al servizio di messaggistica *WhatsApp,* rispetto ai termini esposti nel *Privacy Notice* e alle effettive caratteristiche del servizio; viene anche provata al ricorrenza di concrete ed immediate implicazioni di asimmetria informativa tra gli utenti nonché di esposizione di informazioni fuori contesto.

4. LE NUOVE PROPRIETÀ DEL DATO PERSONALE.

4.1. PROPRIETÀ E POSSESSO DEL DATO PERSONALE. *PERSONAL DATA STORE.*

Proprietà e possesso dei dati personali digitali rappresentano una questione aperta, molto discussa e a tutt'oggi non normata. L'origine della resistenza all'inquadramento regolatorio è costituita dalla nativa immaterialità del dato e dalla sua infinita duplicabilità a costo nullo: ciò rende i dati personali molto diversi dalle *cose* rendendo quindi complicato definire ed esercitare su di essi diritti reali come quello della proprietà.

Ma la sostanziale limitazione non è rappresentata tanto dall'immaterialità (peraltro compensabile dalla natura ontologica dei dati e dalla possibile descrizione semantica) quanto dall'impossibilità di definirne compiutamente l'utilizzo e lo sfruttamento da parte di terzi, condizioni essenziali per regolamentarne il trasferimento, quest'ultimo a sua volta presupposto e implicazione della proprietà di un bene.

Ciò spiega perché altri beni digitali[318] con pari caratteristiche hanno trovato regolamentazioni normative ed implementazioni pratiche non solo per l'assegnazione di un titolo di proprietà ma anche per la sua gestione, la sua protezione e la sua tutela.

Nonostante non ricorrano ancora sistemi che regolino e implementino nella pratica l'assegnazione e l'esercizio del titolo di proprietà sui dati personali tanto nell'ambito normativo tanto in quello delle applicazioni è possibile rintracciare iniziative che per prospettiva ed approccio convergono, pur con delle limitazioni, verso questa direzione.

Dal punto di vista normativo il nuovo Regolamento Europeo 679/2016 eredita e rafforza il diritto (fondamentale) alla protezione dei dati personali consacrandolo come diritto di autodeterminazione esercitabile dall'interessato attraverso diritti di controllo[319]; alcuni di questi diritti – quali il perfezionamento e l'istituzionalizzazione del consenso, il diritto alla limitazione del trattamento ma in particolare il diritto alla portabilità[320] e il diritto alla cancellazione dei dati (Diritto all'oblio)[321], rafforzano il controllo sulle informazioni personali al punto di regolarne decisioni che risulterebbero naturali prerogative di chi sui dati personali

[318] A titolo di esempio si citano le opere di ingegno; libri, musica, immagini in formato digitale; codici e software.

[319] Per i dettagli sull'argomento si rimanda alla trattazione del Capitolo 1 - *Lo scenario normativo attuale. Questioni aperte.*

[320] Cfr GDPR, art. 20 *Diritto alla portabilità dei dati* comma 1. *L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:*<...>

[321] Cfr GDPR, art. 17 *Diritto alla cancellazione («diritto all'oblio»)* comma 1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:* a) *i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;* b) *l'interessato revoca il consenso su cui si basa il trattamento* <...>*;* c) *l'interessato si oppone al trattamento* <...> d) *i dati personali sono stati trattati illecitamente;* <...>

potesse esercitare un diritto di proprietà.

La componente del diritto alla portabilità che ne consente una possibile interpretazione nella direzione della proprietà e del possesso si può cogliere nel considerando 68) del GDPR[322] laddove tale diritto – la cui matrice rimane l'interoperabilità ma esplicitamente declinato strumentale al controllo del dato personale, viene agganciato e subordinato al consenso espresso dall'interessato: è come se il rafforzato istituto del consenso consentisse all'interessato di apporre una caratterizzazione di proprietà/possesso sui propri dati e il diritto alla portabilità ne supportasse l'esercizio salvaguardandone - tramite la standardizzazione del formato e al variare del titolare di trattamento, la riacquisizione e la continuità di utilizzo.

Analoga riflessione può essere fatta per il diritto alla cancellazione strumentale alla completa e definitiva eliminazione dei dati personali e di ogni collegamento ad essi riferibile, decisione dell'interessato interpretabile come una richiesta di definitiva cessazione di trattamento, quindi di condivisione dei propri dati con il titolare quindi, in definitiva, di rientro e ripristino dell'esclusivo utilizzo/possesso del soggetto interessato.

Al rafforzamento del principio di autodeterminazione informativa sancita dal GDPR sul quale prevale – e di fatto limitandolo, la positivizzazione del principio di *accountability* del titolare del trattamento si affianca un ulteriore impulso verso la normazione della proprietà e del possesso dei dati personali introdotto dalla Dichiarazione dei Diritti in Internet[323]. L'art. 5 della dichiarazione richiama ed espone l'essenzialità della tutela del diritto alla protezione dei dati personali contenuta nel Regolamento Europeo, quale premessa per il successivo art. 6 dedicato alla specifica del diritto all'autodeterminazione: *1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano. 2. La raccolta e la*

---

322 Cfr GDPR considerando 68) *Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. <....> Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. <....> Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.*

323 La Dichiarazione dei diritti in Internet, presentata il 28 Luglio 2015, è frutto del lavoro di una Commissione di studio promossa dalla Presidenza della Camera dei Deputati e composta da studiosi, esperti e semplici cittadini che hanno partecipato a una consultazione pubblica, sotto la guida di Stefano Rodotà, con lo scopo di individuare valori fondamentali e principi generali per la nuova cittadinanza digitale. La Dichiarazione anticipa alcuni elementi di novità che saranno successivamente introdotti dal Regolamento: il diritto di accesso alla Rete (art. 2), alla tutela dei dati personali (art. 5), all'autodeterminazione informativa (art. 6) e all'oblio (art. 11).
Il testo integrale della Dichiarazone è inserita in appendice della tesi.

conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata.

Il contesto regolatorio pur direzionandosi verso la configurazione della proprietà e del possesso dei dati personali attraverso forme più robuste di controllo permane carente di un richiamo esplicito a chi ha titolo valido sui dati personali e alla previsione di forme contrattuali per l'utilizzo nel tempo degli stessi.

Questa limitazione trova un possibile superamento e un'accelerazione a supporto di forme di realizzazione del possesso dei dati personali nella implementazione tecnica del *Personal Data Store (PDS).*

Il Personal Data Store/Vault è uno strumento di gestione e memorizzazione di dati personali, risulta componente della metodologia P*ersonal Data Ecosystem*[324] volta centralizzarne il trattamento sull'utente, riconoscendolo principale (se non unico) titolare, decisore e possessore dei propri dati.

Il *PDS* coincide anche con un dispositivo materiale (ad esempio un token interfacciato con una personal application in Cloud) sul quale sono memorizzati i dati personali e le regole necessarie al loro rilascio e utilizzo.

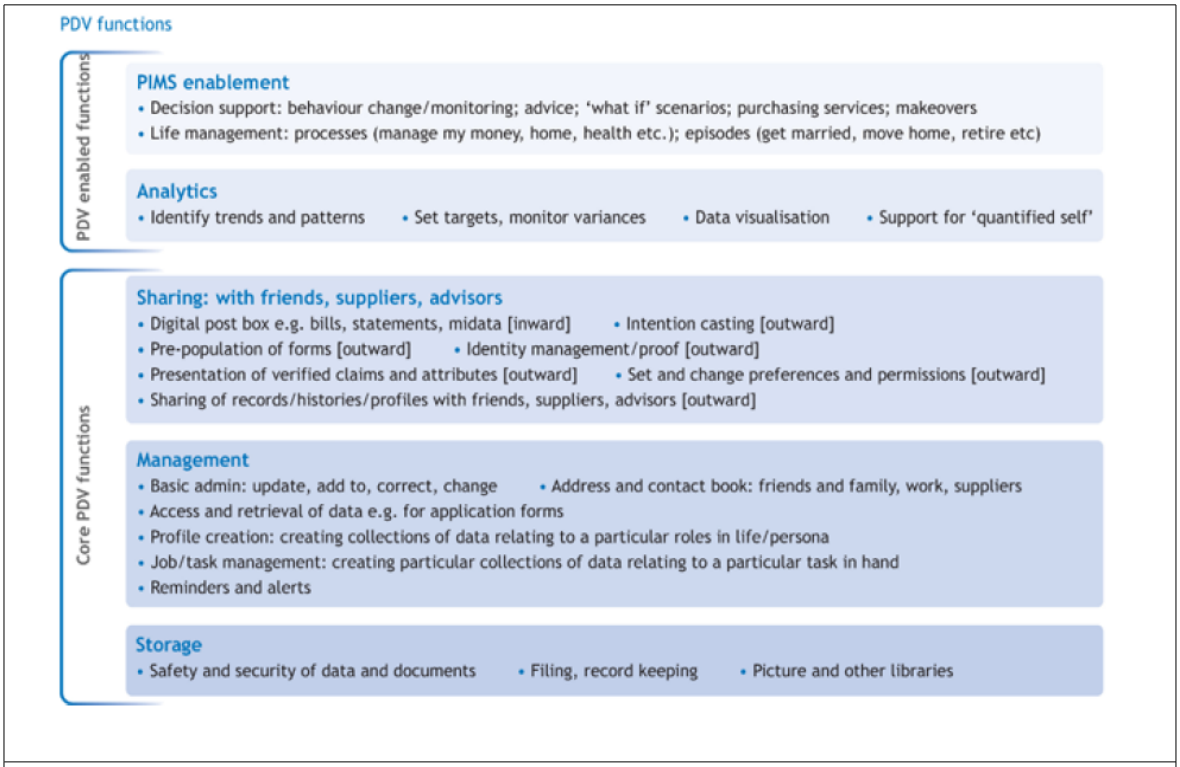


Figura 4.9 – Le funzionalità e i servizi di un *Personal Data Store*[325].

[324] cfr Cavoukian Ann, *Privacy by Design and the Emerging Personal Data Ecosystem* (2012), p 10-13

[325] Fonte Personal Data Stores: A Market Review, Ctrl-Shift 2012, *Privacy by Design and the Emerging Personal Data Ecosystem* (2012), p. 11.

Il *PDS* supporta gli utenti nel raccogliere, memorizzare, utilizzare, condividere, concedere l'accesso a gestire i propri dati personali, fornendo un punto centrale di controllo su informazioni riguardanti gli interessi, i contatti, le affiliazioni, le preferenze, gli amici; la salute, l'istruzione, il patrimonio. Queste possono essere descritte in forma strutturata e non, sotto forma di testo o media (ad esempio file audio, video...).

Il possessore di un *PDS* definisce quali e quanti dati rilasciare per una determinata finalità, il livello di dettaglio o di aggregazione (se in forma grezza, strutturata o aggregata); la portata identificativa: se anonimi o pseudonimizzati; la tipologia di analisi predittive finalizzate a modellare le abitudini, gli aspetti della salute, delle relazioni, della propria immagine e della propria reputazione.

4.2. DATI PERSONALI A SOGGETTI MULTIPLI. *MULTIPLE SUBJECTS PERSONAL DATA.*

L'assenza di meccanismi che pongono un titolo di proprietà dei dati personali sul soggetto interessato implica situazioni di differente distribuzione del controllo, variabile a seconda che i dati personali ricadano nella sfera dei dati identificativi o in quelle più esterne includenti le informazioni fornite volontariamente dall'utente o dedotte da applicazioni di *find engine* o *data mining*[326].

Il soggetto interessato tende a rivendicare un controllo totale o comunque prioritario sui propri dati identificativi diretti o indiretti, percependoli *propri* in ragione del vincolo di attribuzione identificativa. Tuttavia è pur vero che questi dati avrebbero uno scarso margine di utilizzo e di sfruttamento a vantaggio dell'interessato se non fossero trattati (anche commercialmente) da sistemi di gestione sviluppati da altre parti. Queste ultime tendono a rivendicare delle *capabilities* di controllo sui dati, ritenendoli come un vero e proprio bene oggetto di investimenti e presupposto dei relativi ritorni.

Altra considerazione è che di fatto il ciclo di vita e di gestione delle informazioni personali avviene attraverso l'interazione di più parti e l'utilizzo contestuale di dati personali di molteplici soggetti, ciascuno dei quali può esercitare diritti e responsabilità, quindi ricevere conseguenti autorizzazioni.

Si configura quindi uno scenario di diritti, responsabilità, regole d'uso e relative autorizzazioni condivise e non esclusive, riferite ad un contesto necessariamente relazionale e attuabili sulla base del riconoscimento congiunto di più parti.

In questo scenario si colloca una nuova proprietà associabile al dato personale descrittiva dell'essere un dato *multi soggetto*[327].

Si definisce un dato personale multi soggetto – *Multiple Subject Personal Data MSPD,* un dato personale la cui rappresentazione digitale (es. record o set) include identificativi personali (*Personal Identifiable Information, PIIs)* relativi (associabili) a più soggetti. Un *MSPD* può includere:

i. *Identificativi personali PIIs:* sono dati univocamente relativi ai soggetti interessati. La relazione associativa (Personal Data <=> Soggetto) tende ad essere diretta, l'identificazione univoca. Sono esempi il Codice Fiscale, il Nome-Cognome-Data di Nascita; il numero di carta di credito; il MAC Address di un dispositivo; il numero di telefono;…

[326] In argomento per maggior dettaglio sulle tipologie di dati personali si rimanda al precedente capitolo 2 *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità* paragrafo 1.1. *Le proprietà del dato personale, la gestione e gli attori coinvolti.*

[327] Cfr Gnesi Stefania, Matteucci Ilaria, Moiso Corrado, Mori Paolo, Petrocchi Marinella, Vescovi Michele, *My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data,* Privacy Technologies and Policy, Volume 8450 of the series Lecture Notes in Computer Science p. 154-171

ii. Valori diversi dai *PIIs* ma ad essi riconducibili: sono informazioni relative a soggetti i cui *PIIs* sono presenti nel *MSPD*. La relazione associativa (Personal Data <=> Soggetto) tende ad essere indiretta e trovare valorizzazione per il tramite di altre informazioni.

I *MSPD* possono essere raggruppabili in due categorie:

i. *Interazione* – quando contengono parametri che rappresentano esplicitamente la mutua interazione di due o più soggetti. Rappresentano possibili esempi i messaggi SMS o WhatApps; i messaggi di posta elettronica; i record telefonici;

ii. *Co-Localizzazione* – quando contengono parametri di localizzazione che rappresentano la mutua *vicinanza* di due soggetti. Rappresentano possibili esempi i log *DtoD via Bluetooth* oppoure i mutual tagging dei *Social Media*.

Concettualizzare il dato personale associando attributi descrittori contenenti dati identificativi di più soggetti, quindi trattare nativamente il dato come un *Multiple Subject Personal Data* può rivelarsi semplificatore nella modellazione e nella gestione delle regole d'uso.

Su questo aspetto nel capitolo 5 – *Progettazione di un modello di supporto a politiche di privacy user e data centric*, paragrafo 1 – *L'applicazione delle Privacy Policies di tipo User-centric* e paragrafo 1.2. *L'implementazione di una Sticky Privacy Policy per la gestione della lista contatti dell'App di messaggistica WhatsApp Messenger*, viene illustrata una semplice *Proof of Concept* in cui la rubrica contatti di un utente WhatsApp Messenger può essere modellata e trattata come un *Personal Data Store* multi soggetto.

4.3. Il valore economico dei Dati Personali e della *Privacy.*

Il valore economico dei dati personali e della *privacy* è riconducibile ad una costante negoziazione tra sfera pubblica e privata governata da interessi contrapposti tra chi richiede i dati e chi li rilascia, tra benefici e costi.

L'interpretazione della *privacy* anche in termini economici, benché abbia origine e sviluppi recenti[328] in realtà la affianca fin dall'introduzione delle prime coordinate legali, quando le ragioni morali degli avvocati S. Warren e L. Brandeis di invocare il diritto di *essere lasciati (da) soli* trovavano origine e resistenza nel successo commerciale (quindi economico per gli editori) dei primi quotidiani di costume che veicolavano immagini e momenti della vita ritenuti privati.

Il valore associabile ai dati personali e alla loro protezione è una questione associata alla valutazione dei costi e dei benefici connessi alla loro gestione; ma risulta soprattutto legata alla percezione e la consapevolezza tanto dei vantaggi quanto dei rischi di utilizzo che il consumatore è in grado di collocare nel breve e lungo periodo. La misura del valore economico rimane, quindi, una questione fortemente soggettiva, per quanto su di essa incidano elementi misurabili dello *status quo,* delle condizioni di trasparenza e di controllo[329].

Il valore economico della *privacy* può essere rintracciato dietro le motivazioni sollevate a presupposto del presidio delle proprie informazioni personali o, viceversa, a supporto del rilascio dei propri dati personali; le giustificazioni morali che oppongono il rilascio di dati personali o quelle che lo favoriscono, in realtà nascondono o affiancano ragioni economiche - se non monetarie, volte a evitare oneri o a favorire benefici.

Ad esempio la scarsa diffusione su larga scala dei servizi di digitalizzazione dell'identità e del profilo anagrafico al di la delle ragioni tecniche alle quali si ricorre per motivarne l'insuccesso[330], in realtà trova fondamento anche sulla resistenza di molti cittadini ad aderire e a rilasciare le proprie informazioni personali nell'ambito di registrazioni e circuiti digitali con la Pubblica Amministrazione che risulterebbero nativamente condivise ed incrociate nei comparti della sanità, dell'istruzione ma anche del fisco e dei tributi; la retorica della giustificazione morale che oppone il rilascio dei dati personali - invocando ragioni di *privacy,* in realtà maschera

---

328 Cfr Acquisti Alessandro, Privacy, Rivista di Politica Economica, V/VI (2005) p. 343-351

329 Sull'argomento si rimanda al Capitolo 2 - *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità,* Paragrafo 2.4. *Protezione dei dati personali: la centralità dell'utente tra status quo, trasparenza e controllo.*

330 In argomento si segnala *L'insuccesso di Spid è sotto gli occhi di tutti. Intervento di Fulvio Sarzana,* 9 Marzo 2017: *In mancanza di modifiche normative, il Sistema pubblico di identità digitale (SPID) promosso dall'Agenzia per l'Italia Digitale, appare essere un giardino recintato a beneficio di poche imprese a causa del modello utilizzato per la gestione delle attività di identificazione.* Disponibile alla risorsa: https://www.key4biz.it/linsuccesso-spid-gli-occhi-tutti-intervento-di-fulvio-sarzana/183556/

il timore di essere suscettibile a controlli tributari più capillari.

Le stesse ragioni di *privacy* passano, però, in subordine se il rilascio dei dati personali rappresenta contropartita di immediata compensazione monetaria nell'ambito dei servizi offerti da un soggetto privato (cfr successiva figura 4.11).

Per un'impresa il valore dei dati personali di un consumatore è connessa all'abilità di riconoscere e inquadrare il consumatore, proporre prezzi per un bene digitale con un sufficiente margine di certezza che essi saranno accettati.

La misura del valore economico dei dati personali e della loro protezione passa per una valutazione costo-beneficio, il cui esito può essere immediatamente tangibile o differito nel tempo, presentarsi in chiave materiale o essere intangibile; questo differimento riveste un forte peso nell'orientare il comportamento dell'utente/consumatore al rilascio dei propri dati personali o, viceversa, alla loro protezione soprattutto quando condizioni di asimmetria informativa innescano meccanismi di *informazione incompleta* e *razionalità limitata* che precludono al consumatore di valutare compiutamente e nell'immediato se acconsentire o meno al rilascio di dati personali e con quali conseguenze, molte delle quali – tanto per i rischi quanto per i benefici, possono essere scoperte o accertate solo a posteriori.

Il valore dei dati personali e della privacy è rintracciabile nei costi subiti (da consumatori e aziende) quando la privacy viene violata e in quelli sostenuti per presidiare i propri dati.

L'intromissione nella sfera individuale presenta dei costi di invasione riconducibili alle conseguenze dei tipici attacchi dolosi di *cybercrime (*per esempio attuati da virus, malware, pishing; ransomware; da azioni di (DoS - Denial of Service) con danni diretti e immediatamente misurabili come perdita di informazioni[331], furto di identità e di credenziali digitali; ma anche riconducibili agli effetti prodotti da *spamming* e pubblicità spazzatura ricevuta via mail; non secondariamente alla perdita di opportunità per preoccupazioni e sfiducia legate alla gestione della privacy.

Per le aziende il mantenimento della protezione dei dati personali è un costo non solo di gestione - connesso all'acquisto e al mantenimento dei sistemi di contromisure hardware e software e non secondariamente di quelli attinenti la regolamentazione delle politiche e di gestione del consenso, ma anche reputazionale, di immagine e sopratutto di compromissione del patrimonio informativo e della continuità gestionale e operativa in caso di violazioni[332];

[331] Solo per citare il più recente degli esempi in ordine di accadimento, il valore del ripristino dei dati cifrati da *WannaCry 2.0* - il virus ransomware che il 12 Maggio 2017 ha causato una vera e propria epidemia digitale a scopo di ricatto, è pari a 300,00 dollari in bitcoins per ogni utente.

[332] Una stima Eurispes pubblicata da Il Sole 24 Ore domenica 13 maggio in contingenza dell'attacco WannaCry, riferisce

Parimenti il consumatore sostiene dei costi per proteggere i propri dati attrezzandosi di adeguate contromisure (antivirus, sistemi di backup e di perimetrazione,..., e dei relativi oneri di apprendimento per l'utilizzo e il mantenimento); oppure implicitamente subisce dei costi rifiutando il rilascio delle proprie informazioni perdendo così gli eventuali benefici derivanti dalla personalizzazione, dall'accesso a servizi o dal miglioramento della propria *on-line user-experience*.

Anche i benefici che spingono l'utente a sacrificare parte della propria *privacy* possono essere immediati e tangibili, fruibili tramite compensazioni monetarie, sconti o premi; ma altresì essere intangibili e differiti nel tempo.

Ad esempio quando un utente cerca qualcosa su un motore di ricerca diventa attore di una transazione anche se non propriamente finanziaria: rilascia (cede) i propri dati quale contropartita per *trovare* ciò che *cerca,* per *comprare* il risultato della ricerca formulata. I dati rilasciati vengono analizzati, studiati e riutilizzati per servire meglio il consumatore ma anche eventualmente per danneggialo con effetti, conseguenze e tempistica che l'utente non può prevedere (e ai quali forse neppure pensa)[333].

In molti casi anche il consumatore idealmente razionale, assume decisioni sulla protezione dei propri dati personali sottostimandone i rischi e la loro cumulabilità nel tempo, scontando in maniera iperbolica costi e benefici futuri, facendo prevalere i meccanismi di gratificazione immediata su quelli di autocontrollo, eccedendo in ottimismo ritenendo che rischi e violazioni siano un problema altrui.

Quando un utente affronta decisioni sulla protezione dei propri dati raramente dispone di tutti gli elementi per una scelta informata e per una decisione analitica e accurata.

Ma anche in condizioni ottimali di analisi il consumatore potrebbe discostarsi dalla decisione migliore e, per il prevalere di benefici immediati, rilasciare i propri dati con un elevato rischio futuro.

danni per attacchi di hacker alle imprese italiane nel 2solo 016 pari a 9 miliardi di euro.

[333] Per descrivere tale situazione H.R. Varian (1996) usa la metafora dell' *assegno in bianco*, che l'individuo firma quando rivela informazioni personali ad altre parti. Cfr Acquisti Alessandro, Privacy, Rivista di Politica Economica, V/VI (2005) p.332.

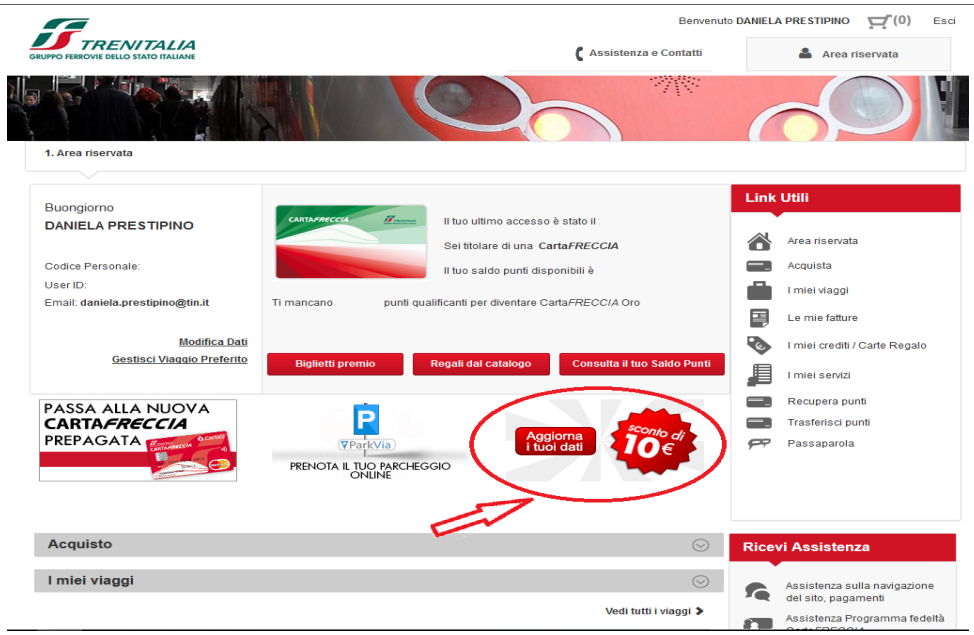


Figura 4.10 – Area riservata del sito Trenitalia-Le frecce: aggiorna i tuoi dati per 10 Euro.
Tra i servizi esposti dal portale rientra quello di poter aggiornare i dati esistenti e già rilasciati in fase di prima registrazione fornendo copia elettronica della propria carta di identità. In caso di adesione il viaggiatore viene immediatamente compensato con uno sconto di Euro 10,00 sull'acquisto di un successivo titolo di viaggio. Analogo premio è previsto nel servizio PassaParola, quando l'utente invita con successo un amico alla registrazione dell'area riservata del portale LeFrecce. Entrambe le forme di compensazione sono ottimi esempi di rilascio e svendita di dati personali, il cui ri-utilizzo è completamente sconosciuto al soggetto interessato.

L'esempio descritto in figura 4.11, per quanto limitato anche nel valore del premio, è significativo perché ben rappresenta quanto possa rivelarsi in un certo senso *sleale* la commercializzazione di dati personali rispetto ad una tradizionale compravendita di beni materiali, in assenza di meccanismi che ne configurano la proprietà[334].

La proprietà di un bene incorpora la possibilità di venderlo ad altri, e il corrispettivo di questa vendita implicitamente (e tra l'altro) dipende dalla conoscenza degli utilizzi associati a questo bene. Non è così in caso di trasferimento di dati personali per i quali il soggetto interessato sconosce l'utilizzo e il ri-utilizzo che ne farà la parte ricevente, con l'inevitabile implicazione di non poterne *fissare il prezzo,* perdendone quindi tanto il controllo informativo tanto quello di valore e di costo.

[334] Cfr precedente paragrafo 4.2 - *Il concetto di possesso e di proprietà del Dato Personale. Personal Data Store.*

CAPITOLO 5

PROGETTAZIONE DI UN MODELLO DI SUPPORTO A POLITICHE DI PRIVACY DI TIPO USER E DATA CENTRIC.

SOMMARIO: 1. L'applicazione delle *Privacy Policies* di tipo *User-centric.* – **1.1.** L'utilizzo delle *Sticky Privacy Policies* per la protezione di un *Multiple Subject Personal Data Store.* – **1.2.** L'implementazione di una *Sticky Privacy Policy* per la gestione della lista contatti dell'App di messaggistica *WhatsApp Messenger.* – **2.** Nuove Ontologie di Dati Personali e di *Privacy.*

1. L'APPLICAZIONE DELLE *PRIVACY POLICIES* DI TIPO *USER-CENTRIC.*

Di seguito si espone un primo caso di studio su *WhatsApp Messenger* di modellazione delle politiche di accesso alle informazioni personali trattate da questa *App,* con la finalità di definire una successiva modellazione di dati personali strumentale affinché le fasi di ragionamento/enforcement/decisione in politiche di controllo degli accessi a dati personali possano risultare più semplificate ed efficaci.

Partendo dalle funzionalità implementate e disponibili in WhatsApp si definiscono esempi di regole "desiderata" di tipo user-centric, che possano indirizzare una rappresentazione (modellazione) del dato personale nativamente (by design) descritta con informazioni (metadati) imprescindibili che consentano al dato personale di essere trattato o utilizzato da più soggetti mantenendone, al contempo, il controllo da parte dell'interessato.

Cosa è WhatsApp Messenger?

WhatsApp Messenger è un'applicazione di messaggistica mobile multi-piattaforma che consente di scambiare messaggi senza pagare gli SMS. *WhatsApp Messenger* è disponibile per i sistemi mobile i*Phone, BlackBerry, Android, Windows Phone e Nokia. WhatsApp* è un'app e come tale legata al sistema operativo dello smartphone sul quale viene eseguita, e in particolare alla rubrica utente in esso configurata.

La messaggistica *WhatsApp* non utilizza il numero di telefono per lo scambio dei messaggi e delle chiamate: il numero di telefono è il prerequisito essenziale per la registrazione e per l'utilizzo del servizio *WhatsApp.* Il numero di telefono associato alla scheda SIM correntemente montata e attiva sullo smartphone può essere diverso da quello fornito in fase di registrazione.

"Entità/Oggetti" WhatsApp

WhatsApp basa il suo funzionamento sulle seguenti entità/oggetto: *i)* profilo utente, *ii)* account utente, *iii)* chat e chiamate, *iv)* notifiche, *v)* contatto e lista contatti WhatsApp, *vi)* contatto telefonico e rubrica telefonica smartphone. Nell'ultima versione rilasciata bel corso del mese di Aprile 2017 è esposto anche lo *stato.*

La rubrica del dispositivo, indipendentemente dal numero di telefono utilizzato - costituisce il *repository* di inizializzazione della lista dei contatti WA. Informazioni di identificazione personale (PII) collezionate e processate da *WhatsApp. WhatsApp* basa il suo funzionamento sul processamento delle seguenti informazioni personali desumibili dal *Privacy Notice*:

a) Numero di telefono di registrazione, immagine personale dell'utente, stato, utenti bloccati: queste informazioni compongono il profilo utente e sono fornite dal soggetto. (per stato si intende un attributo del profilo utente, che può essere libero o valorizzato secondo codifica predefinita, ad esempio: occupato, disponibile, solo chiamate urgenti,…);

b) geo-localizzazione, data e ora ultimo accesso a *WhatsApp,* data, ora e riscontri di lettura, impostazioni di privacy sulla visibilità delle informazioni personali: queste informazioni compongono l'account utente;

c) oltre alle informazioni (applicative) di cui ai precedenti punti, WhatsApp processa numerose altre informazioni identificative l'utente: dati di log e tracciamento quali identificativi dello smartphone o del browser, identificativi di rete.Il perché della scelta *WhatsApp Messenger*

WhatsApp Messenger: Privacy Notice

WhatsApp raccoglie e processa informazioni di identificazione personale, P*ersonal Identification Information – PII,* (es. numero di telefono); informazioni personali (es. stato o ultimo accesso); informazioni personali anonimizzate (es. record dei logs).

Il *Privacy Notice* di *WhatsApp* informa gli utilizzatori del Service e del Site in merito alle informazioni *i)* raccolte e non; *ii)* divulgate/condivise e non; e, *iii) WhatsApp* informa circa l'utilizzo delle informazioni raccolte e/o elaborate. Nell'ordine, in sintesi si riportano i punti più importanti del *Privacy Notice.*

WhatsApp colleziona le informazioni personali - in particolare quelle di identificazione

personale - raccolte dal dispositivo utente (i) o fornite volontariamente dall'utente (ii); queste principalmente includono:

i. la rubrica e la lista contatti del dispositivo telefonico: WhatsApp accede periodicamente (o in esecuzione di una richiesta di aggiornamento lista contatti WhatsApp) alla rubrica del telefono cellulare per individuare i numeri di cellulare di altri account WhatsApp (c.d. numeri/utenti "in-rete"), o comunque categorizzare gli altri numeri di telefono cellulare non corrispondenti ad account WhatsApp (c.d. numeri/utenti "out-rete"), che vengono memorizzati cifrati in modalità irreversibile mediante hash unidirezionali.
ii. il numero di telefono, il nome di notifica, la fotografia personale, lo stato di un utente titolare del profilo (dove per stato si intende un attributo del profilo utente che può essere libero o valorizzato secondo codifica predefinita, ad esempio: occupato, disponibile, solo chiamate urgenti…).

WhatsApp utilizza i tipici oggetti di tracciamento e gestione della sessione: *Cookies* e *Logs*.

WhatsApp dichiara di registrare il numero di clic, i nomi di dominio, le pagine di destinazione, le pagine visitate nonché l'ordine e la quantità di tempo speso su esse, la data e l'ora della richiesta; il browser, il numero di telefono nonché quello dell'utente di cui si richiede lo stato. Inoltre, in obbligazione all'invio o ricezione di messaggi o richieste di visualizzazione e aggiornamento di stato, WsA registra e mantiene informazioni specifiche quali numero di telefono, ora e data.

WhatsApp dichiara di non raccogliere, copiare e mantenere sui propri server:

i. informazioni personali diverse dal numero di telefono incluse e valorizzate nel contatto memorizzato nella rubrica del dispositivo, quali ad esempio email o anagrafica (nome, cognome, alias, immagine del contatto);
ii. i contenuti dei messaggi con esito positivo del ciclo invio-consegna-lettura.

WhatsApp dichiara esplicitamente di divulgare e rendere disponibili nel dominio della propria utenza le informazioni di identificazione personale di un utente - quali lo stato, l'ultimo accesso o ultimo utilizzo dell'applicazione *WhatsApp* - che assumono il carattere di informazioni personali - pubblicamente condivise con gli utenti *WhatsApp* - in ragione dell'inclusione del numero di telefono nella rubrica telefonica del dispositivo smartphone.

WhatsApp dichiara di riservarsi il diritto di divulgare informazioni personali e/o informazioni anonimizzate che ritiene opportune o necessarie per far rispettare i vincoli e i termini di

servizio; e, in via precauzionale, per indagini e difesa contro responsabilità o pretese terze; per aiutare le agenzie governative, per proteggere la sicurezza e l'integrità del sito *WhatsApp* e dei propri server; per proteggere i diritti, la proprietà o la sicurezza di *WhatsApp* e dei suoi utenti.

WhatsApp può raccogliere e condividere informazioni personali anche di identificazione se richiesto per legge o da ragioni riconducibili alla salvaguardia della sicurezza e dell'incolumità di un utente.

WhatsApp dichiara di condividere le informazioni personali con fornitori terzi di servizi nella misura in cui sia ragionevolmente necessario per eseguire, migliorare o mantenere il servizio *WhatsApp*.

WhatsApp può condividere le informazioni personali non identificabili con terze parti interessate per finalità di comprensione dei modelli di utilizzo, servizi, pubblicità..

WhatsApp dichiara di non condividere o vendere – senza il consenso dell'utente esprimibile in modalità *opt-in* o *opt-out* - le informazioni di identificazione personale di un utente con/a società terze per utilizzi commerciali o di marketing.

WhatsApp Site e Service sono servizi ospitati negli Stati Uniti e regolamentati dalle leggi dello Stato della California; l'utilizzo continuato da parte di utenti residenti in paesi con diversa legislazione sulla protezione dei dati personali equivale all'esplicito consenso che le proprie informazioni personali siano trasferite negli Stati Uniti e disciplinate dalle leggi locali.

WhatsApp si riserva, nel caso sia acquisita o fusa con un'entità terza, il diritto di trasferire o assegnare le informazioni raccolte dai nostri utenti come parte di tale fusione, acquisizione, vendita.

1.1. *L'utilizzo delle Sticky Privacy Policies per la protezione di un Multiple Subject Personal Data Store.*

Il record di chiamata telefonica (Call Data Record) è il più tipico esempio di Multiple Subject Personal Data di tipo interattivo. I soggetti possessori del CDR sono per definizione due (Chiamante e Chiamato); entrambi hanno pari diritti di accesso e utilizzo del record che contiene - per definizione e oltre gli attributi propri della chiamata – le informazioni identificative personali dei soggetti: i numeri di telefono. Supponiamo che tali identificativi siano stati configurati nel caso più consueto, ovvero di volontario e reciproco scambio (al momento non entriamo nel merito di casi particolari, ad esempio se uno dei due utenti abbia o meno oscurato il proprio numero). Alla base, inoltre, di un CDR possiamo considerare un record di contatto telefonico formato da due numeri di telefono condivisi nelle due rispettive rubriche. Potremmo definire questo tipo di MSPD simmetrico poiché, l'istanza di un CDR e il corrispondente record di rubrica – nel caso più consueto, pone sullo stesso piano di conoscenza delle informazioni personali entrambi gli utenti, senza intermediari.

Una chat WhatsApp (nell'esempio base di due interlocutori) e i record della relativa lista di contatti sono sovrapponibili ai precedenti esempi - e come tale rappresentano un *Multiple Subject Personal Data* con la differenza, però, che ricorre a priori una *asimmetria informativa*[335].

La condivisione di contatti *WhatsApp* non avviene per scambio volontario ma per il tramite della registrazione al servizio stesso: utilizzando come chiave ricerca primaria il numero di telefono impostato dall'utente in fase di registrazione utente, *WhatsApp* interseca i contatti della rubrica telefonica con i profili *WhatsApp* collezionati sul proprio server ed utilizza il risultato ottenuto per popolare la lista contatti dello specifico profilo *WhatsApp*.

Posto, quindi, che *WhatsApp* costruisce un contatto collezionando le informazioni sia da rubrica dello smartphone (avendone inevitabile accesso) sia da server *WhatsApp*, si creano dei

[335] WhatsApp è una delle applicazioni di messaggistica più contestate in termini di privacy; in argomento si elencano i seguenti riferimenti:
http://www.federprivacy.it/informazione/magazine/1233-in-arrivo-la-terza-qspuntaq-sempre-meno-privacy-suwhatsapp.html
http://www.federprivacy.it/informazione/797-garante-privacy-scrive-a-whatsapp-qcome-utilizzate-di-dati-degli-utenti italianiq.html
http://www.federprivacy.it/informazione/in-primo-piano/1111-ecco-come-la-privacy-su-whatsapp-e-a-rischio.html
http://espresso.repubblica.it/visioni/tecnologia/2014/11/07/news/whatsapp-altro-che-doppia-spunta-blu-ecco-perche-e-a-rischio-la-privacy-1.187132
http://www.repubblica.it/tecnologia/sicurezza/2015/06/19/news/whatsapp_sicurezza_colabrodo-117221628/?refresh_ce
http://www.panorama.it/mytech/sicurezza/whatsapp-e-la-peggiore-nel-proteggere-la-nostra-privacy/
http://www.tuttoandroid.net/android/whatsapp-viola-la-privacy-degli-utenti-tutti-i-dettagli-sulla-vicenda-90155/
Le critiche mosse condividono come le impostazioni di default di WhatsApp espongano l'utente (inconsapevole) ad una condivisione delle proprie informazioni personali sostanzialmente pubblica sia per attributi del profilo sia per geolocalizzazione e avvenuta lettura del messaggio.

disallineamenti (o asimmetrie) tra le due fonti che l'utente proprietario del profilo *WhatsApp* (reso edotto, informato e consapevole) potrebbe conciliare definendo delle regole.

WhatsApp Messenger: Esempi di politiche di accesso e utilizzo delle entità

Esempio 1

a) Alice acquista il suo primo smartphone *Android* con integrato una scheda telefonica Sim anch'essa di prima attivazione. Deve attivare un account Google; decide di scaricare *WhatsApp Messenger* sul suo smartphone.

b) Utilizza il numero associato alla Sim per registrarsi a *WhatsApp;* dopo aver spuntato l'accettazione del *Privacy Notice* attiva il suo profilo che personalizza con immagine e stato.

c) Alice sottovaluta le impostazioni di privacy, di visibilità e condivisione delle informazioni perché le ignora non essendo stata informata in maniera esplicita.

d) Su questi presupposti: Alice è un utente *WhatsApp,* la rubrica del nuovo smartphone è vuota così come lo sarà la lista contatti associata al suo profilo *WhatsApp.*

e) Alice importa sul nuovo *smartphone* il file Rubrica_Alice.vcf estratto dal vecchio cellulare-

f) Alice aggiorna la lista contatti *WhatsApp* che improvvisamente si popola di amici e conoscenti (ma anche di contatti sostanzialmente sconosciuti) recenti e non, con relative foto e immagini.

g) Alice ha litigato con Bob e vorrebbe cancellare il suo contatto dalla lista WhatsApp, pur mantenendolo nella propria rubrica: questa opzione non è implementata.

h) Alice vorrebbe inviare un messaggio *WhatsApp* (non anonimo) a Bob, ma preferirebbe oscurare il nuovo numero

Asimmetria informativa:

Alice conosce molte più informazioni sui suoi contatti WhatsApp di quanto quest'ultimi conoscono del suo profilo praticamente nulla, non essendo Alice nella loro lista contatti *WhatsApp* poiché il nuovo numero di Alice (non ancora diffuso) non risulta registrato nelle rispettive rubriche telefoniche.

Politiche esempio 1 (funzionalità WhatsApp: Aggiorna)

1. Quando aggiorni la *lista_contatti_WhatsApp* di Alice popola la lista con i profili di utenti WhatsApp nella cui rubrica telefonica è inserito il numero di telefono di Alice.
2. Quando aggiorni la *lista_contatti_ WhatsApp* di Alice cancella, se presenti, contatti che hanno cancellato il contatto di Alice nella propria rubrica telefonica.
3. Consenti ad Alice di eliminare un contatto *WhatsApp* pur mantenendolo nella rubrica telefonica
4. Quando invii una chat *WhatsApp* il cui destinatario non ha ancora il numero di telefono del utente mittente, consenti a quest'ultimo di optare per la visibilità o l'oscurazione del proprio numero.

Esempio 2

a) Alice non condivide di non essere inclusa dalla lista contatti *WhatsApp* dei suoi contatti telefonici;

b) Alice modifica il numero telefonico del suo profilo *WhatsApp* inserendo il vecchio, quello diffuso ad amici e conoscenti.

c) Riceve subito molte chat, compresa quella di Bob;

d) Alice è sorpresa poiché aveva precedentemente aggiunto Bob nell'elenco dei contatti rifiutati e vorrebbe mantenere l'impostazione senza preoccuparsi di riconfigurare l'opzione anche per la lista contatti di *WhatsApp*

Asimmetria informativa:

Alice di fatto riceve comunicazione non desiderate.

Politiche esempio 2 (funzionalità WhatsApp: Aggiorna)

1. Se il contatto di un utente è bloccato nella rubrica del telefono di Alice allora non includere il contatto nella lista *WhatsApp;* oppure (sotto analoga condizione) chiedi conferma.
2. Viceversa: Se blocchi un utente incluso nella lista contatti *WhatsApp* di Alice allora blocca il corrispondente contatto inserito nella rubrica (o chiedi conferma).

Esempio 3

a) Alice scorre la sua lista contatti di *WhatsApp* e rileva molti profili di scarso interesse che non riconduce a distinti e identificati soggetti;

b) eppure di questi contatti visualizza immagini ed informazioni di stato sostanzialmente non desiderati. Deduce che può accadere anche il viceversa ovvero che anche questi contatti visualizzino le informazioni del suo profilo.

c) Alice restringe la visibilità del suo profilo a tutti e i soli contatti della lista, ma vorrebbe escluderne alcuni e limitarne altri.

Politiche esempio 3 (funzionalità WhatsApp: Impostazioni.Account.Privacy)

Per ogni contatto della lista WhapsApp proponi e consenti ad Alice:

1. Di scegliere quali informazioni di profilo e di account esporre: immagine, stato, accesso, avvenuta lettura delle chat.
2. Viceversa: in coerenza alle impostazioni di accesso e visibilità dei suoi contatti scegliere quali, delle informazioni esposte e rilasciate, trattenere ed visualizzare nella propria lista contatti.
3. Configurare la durata temporale dei filtri.

Esempio 4-5

a) Alice riflette che parte della sua rubrica smartphone è ben organizzata: i contatti più utilizzati e quelli degli amici più stretti sono molto dettagliati e valorizzati in tutti gli attributi accessori (es. Alias, Email, Organizzazione, pagina web, numeri telefonici secondari....), oltre che essere già organizzata in gruppi (es. Famiglia, Amici, Lavoro....).

b) Non altrettanto i corrispondenti contatti inclusi nella lista WhatsApp e ciò perchè WhatsApp ha dichiarato esplicitamente l'esclusione di tali informazioni dal suo utilizzo.

c) Inoltre Alice vorrebbe utilizzare WhatsApp solo con sottoinsiemi di contatti già presenti nella rubrica del proprio smartphone.

Asimmetria informativa:

Disallineamento delle fonti informative rispetto alla medesima finalità e utilizzo: scambiare messaggi e chiamate.

Politiche esempio 4

Per ogni contatto della lista *WhapsApp* proponi ad Alice sul proprio smarthphone:

1. di collegare il contatto *WhatsApp* alla corrispondente entry della rubrica del proprio smartphone.
2. Oppure di ereditarne tutte le informazioni personali.
3. Di inserire informazioni aggiuntive quali ad esempio: la programmazione per data e ora di una chat.
4. Di pre-impostare dei gruppi di chat.

Politiche esempio 5 (funzionalità WhatsApp: Impostazioni.Account, Aggiorna)

Nelle impostazioni di account consenti ad Alice di definire delle regole, ad esempio:

1. Quando aggiorni la lista contatti includi solo i contatti telefonici con maggiore frequenza di comunicazione (es. nell'ultimo mese).
2. Oppure solo quelli di gruppi già presenti in rubrica: es. solo Familiari o solo Amici
3. Escludi o chiedi conferma per i contatti inseriti in rubrica con i quali non intercorrono comunicazioni da oltre <*filtro*>
4. Aggiorna la lista contatti con gli utenti geolocalizzati <*filtro*>

Esempio 6

a) Alice consulta il suo account Google drive.

a) Rileva vari backup di dati e informazioni al contempo memorizzate sul suo smartphone, compreso quello di WhatsApp: chat criptate e media scambiati in chiaro quali video, immagini e immagini di profilo dei contatti.

a) Nessun alert ha informato Alice del download automatico sul proprio dispositivo delle immagini dei profili, e in analogia anche della propria immagine di profilo sui

dispositivi di altri Account.

Asimmetria informativa:

Perdita di controllo sul proprio dato personale

Politiche esempio 6 (funzionalità WhatsApp: Impostazioni.Account,Privacy; Impostazioni.Profilo)

1. Quando configuri il profilo proponi e consenti ad Alice di configurare gli attributi di utilizzo della propria immagine icona del profilo: es. Visibile (e non); Salva (e non).
2. Notifica ad Alice se un utente dei suoi contatti ha associato una immagine al suo profilo.

Ulteriori esempi di politiche

Ulteriori esempi, atteso che *WhatsApp* ha imprescindibile e inevitabile accesso non solo alla rubrica ma anche alla memoria dello smartphone, possono coprire le Notifiche e l'utilizzo dello Stato per filtrare alcune azioni. Ad esempio:

1. Se lo Stato è "Disponibile" passa chat e chiamate
2. Se lo Stato è "In riunione" sospendi la chat per un pre-determinato intervallo di tempo.

1.2 L'implementazione di una Sticky Privacy Policy per la gestione della lista contatti dell'App di messaggistica WhatsApp Messenger.

TrustedPhoneBook (TPB) - Specifiche tecniche e funzionalità

Descrizione

TrustedPhoneBook (TPB, nel seguito questo il riferimento per brevità) è un'App (per Android) che consente all'utente proprietario di uno smarphone e sottoscrittore del servizio di WhatsApp Messenger di filtrare i contatti della propria rubrica da esporre a WhatsApp (nel seguito); quindi il proprietario di una rubrica - impostandone la visibilità degli attributi, controlla il disclosure della propria rubrica a WA e la divulgazione/visibilità del proprio profilo nella comunità degli utenti WA.

Il servizio parte da questo presupposto: WA costruisce un contatto ricavando informazioni sia da rubrica dispositivo (avendone inevitabile accesso) sia da server WA; si rilevano dei disallineamenti tra le due fonti, che l'utente proprietario del profilo WA potrebbe conciliare definendo delle regole, che tradotte sotto forma di *Sticky Policies* possono essere associate/attaccate alla rubrica personale.

WA accede alla rubrica dell'utente dopo l'enforcement e l'esecuzione delle Sticky Privacy Policies, il cui risultato è un sottoinsieme di rubrica coerente con le preferences configurate dall'utente.

L'architettura consta di due parti: - *TPB-server,* e *TPB-App,* e 4 moduli applicativi. Il servizio presuppone: *i)* la registrazione dell'utente che scarica l'App ad un servizio di repository fidato erogato dal server; *ii)* la sincronizzazione della rubrica dello smarphone su un cloud (es. Drobox, Google Drive). L'implementazione presuppone di utilizzare come chiave primaria l'hash del numero telefonico di tutti i sottoscrittori di cui al punto *i).*

Modulo 1, TPB-server:

1. Scarica l'app sullo smartphone dell'utente;

2. Tramite elementi grafici, fornisce all'utente un'informativa molto semplice dell'esposizione del profilo telefonico in WhatsApp in termini di informazioni necessarie o visibili, rispetto alla finalità del servizio di messaggistica, e le relative implicazioni. Esempio:

Il mio numero tel.	Necessario	Visibile	Implicazione
Quando è inserito nella rubrica di un contatto	no	si	Impossibilità di oscurare il (mio) numero nel profilo WA del contatto.
Quando è inserito nella rubrica telefonica di un utente che non è contatto della propria rubrica	si	si	Impossibilità di impedire la visibilità del (mio) profilo in profili di utenti che non sono (miei) contatti.
In relazione ai contatti bloccati	//	si	Impossibilità di oscurare/cancellare un contatto bloccato in rubrica

Modulo 2, TPB-App

(Input rubrica; Output rubrica + sticky policy associata alla rubrica)

A) Per il numero dell'utente e per ogni contatto in rubrica consente di impostare semplici regole di visibilità. Esempio di regola nella *Sticky Policy* di un utente A[336]

1. condizione necessaria e sufficiente perché il numero di A sia incluso nella lista contatti WhatsApp di un altro utente è che il numero di telefono di quest'ultimo sia già nella rubrica telefonica di A. Ad esempio:
   a) Se il B è un contatto di A (quindi utente B è in rubrica di A) e A è un contatto di B allora mantieni il numero di B nella rubrica di A da rilasciare a WA[337]. Quindi deriva un'altra regola:
   b) Se B non è un contatto di A (quindi utente B non è in rubrica di A) ma A è un contatto di B allora non inserire il numero di A nella rubrica di B da rilasciare a WA.
2. condizione necessaria per il popolamento della lista contatto WhatsApp è che i numeri di telefono non siano stati bloccati nella rubrica. Ad esempio:
   a) Se B è un contatto bloccato di A (quindi utente B è in rubrica di A) allora non inserire il numero di A nella rubrica di B da rilasciare a WA.

336 Si presuppone che A e B siano utenti WA

337 Può valere il viceversa per la Sticky Policy di B.

3. seleziona (oppure escludi) i seguenti contatti dalla mia rubrica da includere nella lista contatti di WhatsApp. Ad esempio:
   a) Se B è un contatto preferito di A (quindi utente B è in rubrica di A) allora mantieni il numero di B nella rubrica di A da rilasciare a WA[2]
   b) Se B è un contatto di A (quindi utente B è in rubrica di A) allora mantieni B nella lista contatti di A per un tempo prefissato, es. dal 01 gennaio al 31 gennaio.

B) **TPB-App** trasforma le impostazioni in una Sticky Privacy Policy
// machine-readabe, tramite XML RDF

Modulo 3, TPB-App:

(Input: rubrica + sticky policy associata alla rubrica + credenziale di identificazione.

Output: creazione del package dati firmato digitalmente)

1. Costruisce il package dati firmato digitalmente contenente la rubrica dell'utente e la associata sticky policy.
2. Trasmette il package al modulo 4

Modulo 4, TPB-Server:

(Input: package dati firmato digitalmente.

Output: Sottoinsieme della rubrica da condividere con WhatsApp)

Per ogni package ricevuto:

1. Scompone e verifica il package
2. Estrae la rubrica e la sticky policies
3. Per ogni entries di rubrica incrocia e applica le rispettive sticky policies, eliminando i contatti che non le verificano.
4. Invia al dispositivo dell'utente o al cloud da egli indicato la nuova rubrica

2. NUOVE ONTOLOGIE DI DATI PERSONALI E DI PRIVACY.

Il volume dei *Big Data* inteso come ampiezza semantica punta a incrociare la dimensione quantitativa e quella qualitativa del dato, nella misura un cui algoritmi sono sempre più in grado di comprendere il dato, estrarre le relazioni semantiche con gli altri dati, ricavare nuova informazione mediante attributi ritenuti pertinenti e attendibili (componente qualitativa), all'interno di una mole crescente di dati (componente quantitativa).

Lo schema *Big Data* è un meccanismo di arricchimento dei dati, basato su metadati e attributi descrittori. Qualsiasi sistema di ragionamento sui dati, comprese le regole di utilizzo definite dall'utente, passa dai dati stessi e dalla capacità di caratterizzarli affinché espongano proprietà che facilitino in maniera dinamica al contesto, il controllo d'uso da parte dell'utente; dove - in esito ai nuovi scenari si vulnerabilità e di rischio esposti nel precedente capitolo 4 - Ver*so la Privacy 2.0: nuovi scenari di rischio e nuove semantiche* per controllo d'uso si possa intendere la ottimale prevenzione delle stesse intervenendo *by design* sul miglioramento e il mantenimento della qualità del dato o comunque evitandone il degrado.

La limitazione sulla concettualizzazione di dato personale e alla sua caratterizzazione, come illustrato nel capitolo 2 della tesi - *Privacy e Protezione dei Dati personali: pluralità semantiche e criticità* è connessa al fatto che tale concettualizzazione è legata ad una definizione assolutamente generale, ad una altrettanto ampia definizione di trattamento ma al contempo ad un'assenza di modellazione legata alla finalità (se non per la sommaria distinzione in finalità primarie e secondarie) e alla tipologia di dato. La risposta – secondo le fonti disamine in letteratura e già indicate al capitolo 2, potrebbe essere rintracciata nel modellare il dato personale in un contesto parametrizzato dallo stesso piuttosto che dalle caratteristiche di trattamento, rendendo così possibile configurare diritti, responsabilità e quindi permessi (intesi quali azioni applicative di diritti e responsabilità) in maniera adattabile, flessibile ma soprattutto dinamicamente dipendente dalle finalità e dall'utilizzo.

Ciò può essere ottenuto prevedendo metadati descrittivi che alla specifica della tipologia e alla distinzione della finalità[338] affiancano la tipologia di *collezionamento* (dati volontari, osservati e dedotti), il *formato* (grezzi, aggregati e visualizzati) gli indicatori di qualità: esattezza e correttezza, pertinenza, accuratezza, completezza, non-ridondanza, validità temporale;

[338] Il tipo distingue i dati a seconda del coefficiente di privatezza o confidenzialità percepito dall'utente; ad esempio in genere sono ritenute private le informazioni finanziarie, o alcune informazioni non sensibili ma attinenti la salute. La finalità attiene la distinzione in finalità primaria e secondaria (ulteriore) del trattamento. In entrambi i casi sono caratteristiche che itervengono in maniera molto sommaria nella specificazione del trattamento piuttosto che nella concettualizzazione del dato personale in quanto tale.

coerenza e appropriatezza nonché quelli attinenti le nuove proprietà: *dato multi-soggetto*, la *proprietà,* il *valore.*

Gli attributi relativi al ***collezionamento*** descrivono una sorta di spettro dei dati stessi rispetto alla contrapposta percezione di controllo del soggetto interessato e del titolare al trattamento; caratterizzano il dato personale in:

- ✔ *volontario* – fornito o creato direttamente dall'utente, quindi *la mia* foto, *la mia* immagine, *il mio* post, oltre che gli identificatori come *il mio* email, *il mio* nome;
- ✔ *osservato* – risultato di transazioni tra l'utente e un titolare di trattamento, quindi ad esempio trovano descrizione dati di geolocalizzazione, tracciamento di acquisti, di attività on-line o di rete; e
- ✔ *dedotto* – derivati dalla combinazione analitica delle prime due tipologie; questo attributo descrive la ricorrenza di derivata informazione e nuova conoscenza.

Il passaggio da *volontari – osservati – dedotti* traccia un gradiente di controllo inversamente proporzionale tra gli utenti e i titolari al trattamento in cui si può inserire l'attributo descrittivo della proprietà/possesso, quindi della compresenza sullo stesso dato di più soggetti interessati (dato multisoggetto): più i dati evolvono verso i *dedotti,* più i titolari - che su quelle deduzioni investono risorse, tempo e tecnologia, tendono a ritenerli propri (un proprio *asset).*

Gli utenti invece tendono a percepire un forte senso di proprietà e prerogativa di controllo individuale verso i dati *volontari.* I dati *osservati* in un certo senso migrano la percezione di controllo verso i titolari nella misura in cui questi più che sfruttarli li intercettano e li registrano; non assumendo evidente e immediato impatto sulla personalità dell'utente, questi tende a delegarne la gestione ai titolari. Al diminuire del controllo corrisponde, per l'utente, una speculare percezione di aumento del rischio di pericolo e danno per le proprie informazioni.

Gli attributi descrittivi il formato caratterizzano il dato personale in:

- ✔ *dato grezzo,* la cui valorizzazione rappresenta la misura e il formato in cui sono stati raccolti, privi di codifica e analisi;
- ✔ *dato aggregato* o *estratto,* la cui valorizzazione rappresenta la ricorrenza di analisi statistiche di base, prettamente quantitative;
- ✔ *dato visualizzato,* la cui valorizzazione rappresenta la combinazione dei precedenti e la

ricorrenza di analisi sia quantitative più complesse, che qualitative.

Infine gli attributi descrittivi la qualità dei dati caratterizzano il dato per gli indicatori di: *esattezza* e *correttezza, pertinenza, accuratezza, completezza, non-ridondanza, validità temporale; coerenza e appropriatezza.*

La caratterizzazione della *privacy* risulta completata da ulteriori proprietà inserite e schematizzate nella figura 5.1 che segue: la qualità dei dati, il contesto dei dati (lo scenario), la proprietà, nuovi rischi, le reazioni comportamentali del soggetto interessato.

Il controllo d'uso potrebbe essere implementato mediante l'applicazione di infrastrutture di *Digital Rights Management* - rivedute e riutilizzate sul dato personale, volte a fornire controllabilità, auditability e trasparenza sul governo e l'assicurazione delle informazioni personali – in equivalenza alla riservatezza, all'integrità e alla disponibilità.

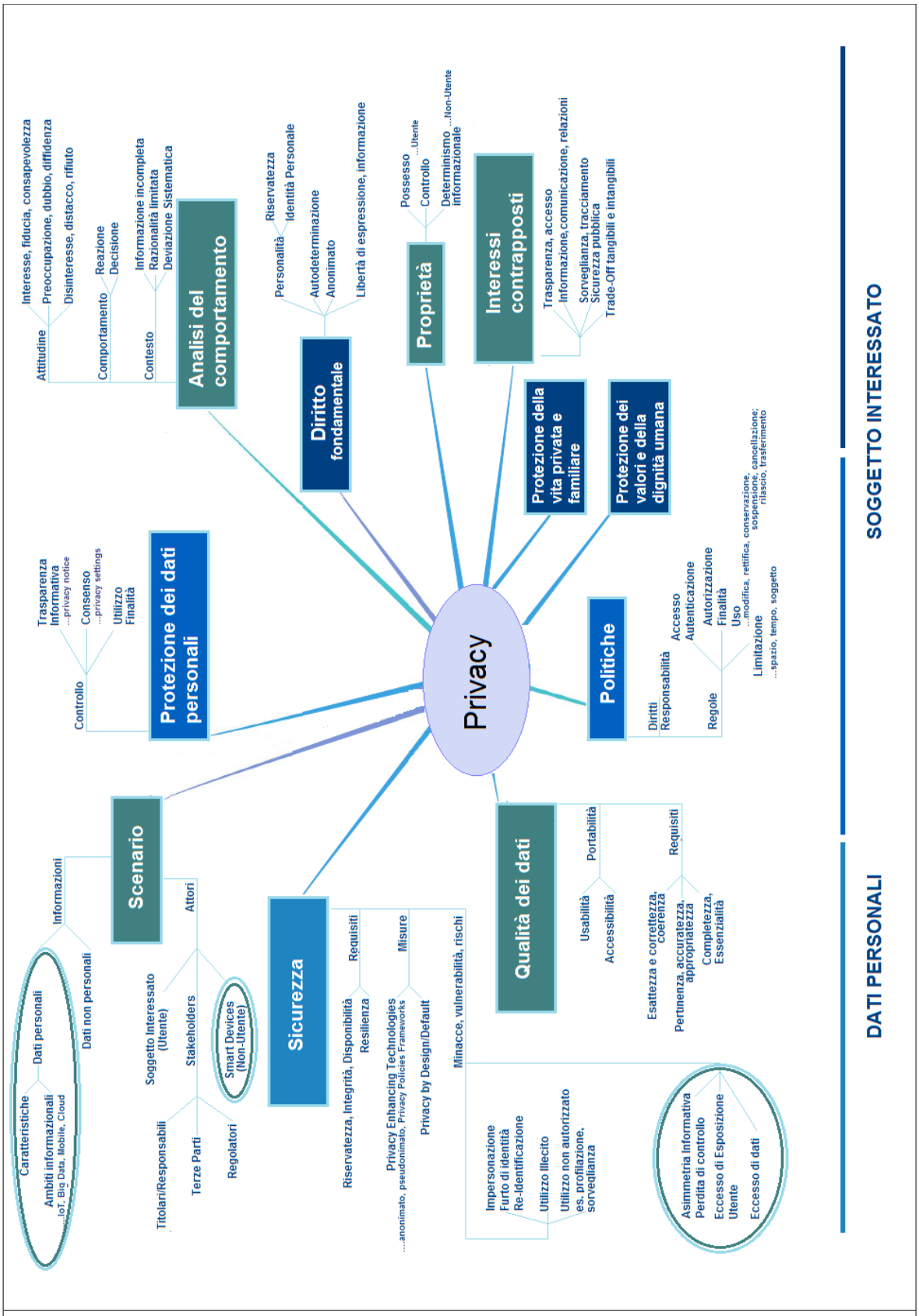


Figura 5.1. - Nuova Modellazione della Privacy

CONCLUSIONI

Questa tesi di Dottorato – *Nuovi scenari di rischio e misure user-centric per la protezione dei dati personali,* ha discusso la centralità degli utenti nei processi di gestione della *privacy* e della protezione dei dati personali; ha proposto e sostenuto un modello concettuale e applicativo basato su politiche *users-centric* di tipo *Sticky Privacy Policies* per un *efficace* e *dinamico* controllo contestuale del trattamento e della divulgazione dei dati personali, in contesti informazionali distinti dalle seguenti questioni aperte:

1. la ricalibrata centralità del soggetto interessato che si qualifica quale principale produttore di informazioni personali/identificative/private che diventano pubbliche per impostazione predefinita *(default settings)* e, come tali, origine di violazioni non previste;
2. la contestuale criticità per l'utente di controllarne il ri-utilizzo durante il ciclo di vita del trattamento che, sempre più allocato in contesti informazionali *multi soggetto* e *data intensive,* processa e relaziona volumi di dati personali per finalità e utilizzi secondari differenti rispetto a quelli associati all'iniziale rilascio.

La ricerca ha tenuto conto sia delle prescrizioni regolatorie giuridiche allo stato vigenti sia di quelle tecniche, rilevandone le relative limitazioni; quindi degli standard applicativi *de facto* in materia di *privacy framework*.

Partendo dall'analisi del ricalibrato ruolo del soggetto interessato quale principale produttore di dati personali, *intrinsecamente* pubblici e condivisi per *default settings* e dalle implicazioni sul ridisegno di una sfera privata sempre più confusa e sovrapposta a quella pubblica, sono state individuate dieci nuove forme di vulnerabilità e di rischio:

1. l'asimmetria informativa tra chi produce le informazioni e chi le sfrutta;
2. il mantenimento degli indicatori di qualità del consenso nel suo configurarsi informato, libero, specifico, inequivocabile e concludente;
3. la dispersione e la perdita di controllo sulle dati personali;
4. l'eccesso di dati personali (ridondanza e massimizzazione quantitativa nell'utilizzo dei dati personali);
5. la molteplicità e il proliferare finalità di utilizzo incontrollate;
6. il difetto di trasparenza;
7. l'eccesso di esposizione del soggetto interessato,
8. la deduzione invasiva di attitudini e aspetti della personalità;

9. oltre a vulnerabilità collegabili alla pluralità dei titolari componenti la filiera degli stakeholders; e
10. alla scarsa nativa compliance *privacy by design/default* dei trattamenti.

Queste nuove vulnerabilità sono coerenti con una valutazione di rischio *ex-ante* al trattamento, riconducibili ad un degrado di qualità e opponibili con misure di *privacy by design.*

Il progetto propone una semplice *Proof of Concept* a supporto della validità delle argomentazioni precedenti utilizzando come contesto applicativo l'App *WhatsApp Messenger,* assumendo la rubrica contatti di un utente *WhatsApp* come un *Personal Data Store* a soggetti multipli (*Multiple Subjects Personal Data Store*), definendo un modello implementativo di supporto basato sull'utilizzo di *Sticky Privacy Policy* in cui vengono intersecate le regole d'uso di ogni utente. In particolare viene posta in risalto il ricorrere di asimmetria informativa, perdita di controllo ed eccesso di esposizione per l'utente.

In chiusura viene proposto un set di nuovi descrittori semantici associabili ad altrettante proprietà del dato personale – il *collezionamento,* il *formato,* attributi di qualità oltre a nuove proprietà: *dato multi soggetto, proprietà* e *valore* – affinché la modellazione ricavabile supporti, in prospettiva, una ottimale gestione contestuale della *privacy* basata su regole *user e data centric.*

In tale contesto può trovare collocazione una nuova modellazione concettuale della *privacy* stessa volta - quale controllo d'uso, al mantenimento dei requisiti di *controllabilità, auditability* e *trasparenza* sul governo e l'assicurazione delle informazioni personali – ad estensione e superamento dei tradizionali ed equivalenti requisiti di riservatezza, integrità e disponibilità.

Quest'ultimo punto risulta il presupposto di sviluppi futuri del progetto connessi alla definizione di una vera e propria ontologia di *privacy* includente la necessaria elencazione, il dettaglio, la relazione delle proprietà introdotte e la relativa valorizzazione degli di attributi descrittivi.

Dichiarazione dei diritti in Internet

Questo documento costituisce **il nuovo testo della Dichiarazione** elaborato dalla *Commissione per i diritti e i doveri relativi ad Internet* a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015.

Preambolo

Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet deve essere considerata come una risorsa globale e che risponde al criterio della universalità.

L'Unione europea è oggi la regione del mondo dove è più elevata la tutela costituzionale dei dati personali, esplicitamente riconosciuta dall'articolo 8 della Carta dei diritti fondamentali, che costituisce il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale.

Questa Dichiarazione dei diritti in Internet è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale. Internet si configura come uno spazio sempre più importante per l'autorganizzazione delle persone e dei gruppi e come uno strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale.

I principi riguardanti Internet tengono conto anche del suo configurarsi come uno spazio economico che rende possibili innovazione, corretta competizione e crescita in un contesto democratico.

Una Dichiarazione dei diritti di Internet è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale.

Art. 1.

(Riconoscimento e garanzia dei diritti).

1. Sono garantiti in Internet i diritti fondamentali di ogni persona riconosciuti dalla Dichiarazione universale dei diritti umani delle Nazioni Unite, dalla Carta dei diritti fondamentali dell'Unione Europea, dalle costituzioni nazionali e dalle dichiarazioni internazionali in materia.

2. Tali diritti devono essere interpretati in modo da assicurarne l'effettività nella dimensione della Rete.

3. Il riconoscimento dei diritti in Internet deve essere fondato sul pieno rispetto della dignità, della libertà, dell'eguaglianza e della diversità di ogni persona, che costituiscono i principi in base ai quali si effettua il bilanciamento con altri diritti.

Art. 2.

(Diritto di accesso).

1. L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.

3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.

4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.

5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità

Art. 3.

(Diritto alla conoscenza e all'educazione in rete).

1. Le istituzioni pubbliche assicurano la creazione, l'uso e la diffusione della conoscenza in rete intesa come bene accessibile e fruibile da parte di ogni soggetto.

2. Debbono essere presi in considerazione i diritti derivanti dal riconoscimento degli interessi morali e materiali legati alla produzione di conoscenze.

3. Ogni persona ha diritto ad essere posta in condizione di acquisire e di aggiornare le capacità necessarie ad utilizzare Internet in modo consapevole per l'esercizio dei propri diritti e delle proprie libertà fondamentali.

4. Le Istituzioni pubbliche promuovono, in particolare attraverso il sistema dell'istruzione e della formazione, l'educazione all'uso consapevole di Internet e intervengono per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di Internet da parte delle persone.

5. L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla Rete tra attori economici, Istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.

Art. 4.

(Neutralità della rete).

1. Ogni persona ha il diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone.

2. Il diritto ad un accesso neutrale ad Internet nella sua interezza è condizione necessaria per l'effettività dei diritti fondamentali della persona.

Art. 5.

(Tutela dei dati personali).

1. Ogni persona ha diritto alla protezione dei dati che la riguardano, per garantire il rispetto della sua dignità, identità e riservatezza.

2. Tali dati sono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili

3. Ogni persona ha diritto di accedere ai dati raccolti che la riguardano, di ottenerne la rettifica e la cancellazione per motivi legittimi

4. I dati devono esser trattati rispettando i principi di necessità, finalità, pertinenza, proporzionalità e, in ogni caso, prevale il diritto di ogni persona all'autodeterminazione informativa.

5. I dati possono essere raccolti e trattati con il consenso effettivamente informato della persona interessata o in base a altro fondamento legittimo previsto dalla legge. Il consenso è in via di principio revocabile. Per il trattamento di dati sensibili la legge può prevedere che il consenso della persona interessata debba essere accompagnato da specifiche autorizzazioni.

6. Il consenso non può costituire una base legale per il trattamento quando vi sia un significativo squilibrio di potere tra la persona interessata e il soggetto che effettua il trattamento.

7. Sono vietati l'accesso e il trattamento dei dati con finalità anche indirettamente discriminatorie.

Art. 6.

(Diritto all'autodeterminazione informativa).

1. Ogni persona ha diritto di accedere ai propri dati, quale che sia il soggetto che li detiene e il luogo dove sono conservati, per chiederne l'integrazione, la rettifica, la cancellazione secondo le modalità previste dalla legge. Ogni persona ha diritto di conoscere le modalità tecniche di trattamento dei dati che la riguardano.

2. La raccolta e la conservazione dei dati devono essere limitate al tempo necessario, rispettando in ogni caso i principi di finalità e di proporzionalità e il diritto all'autodeterminazione della persona interessata.

***Art.** 7.*

(Diritto all'inviolabilità dei sistemi, dei dispositivi e domicili informatici).

1. I sistemi e i dispositivi informatici di ogni persona e la libertà e la segretezza delle sue informazioni e comunicazioni elettroniche sono inviolabili. Deroghe sono possibili nei soli casi e modi stabiliti dalla legge e con l'autorizzazione motivata dell'autorità giudiziaria.

Art. 8.

(Trattamenti automatizzati).

1. Nessun atto, provvedimento giudiziario o amministrativo, decisione comunque destinata ad incidere in maniera significativa nella sfera delle persone possono essere fondati unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

Art. 9.

(Diritto all'identità).

1. Ogni persona ha diritto alla rappresentazione integrale e aggiornata delle proprie identità in Rete.

2. La definizione dell'identità riguarda la libera costruzione della personalità e non può essere sottratta all'intervento e alla conoscenza dell'interessato.

3. L'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano.

4. Ogni persona ha diritto di fornire solo i dati strettamente necessari per l'adempimento di obblighi previsti dalla legge, per la fornitura di beni e servizi, per l'accesso alle piattaforme che operano in Internet.

5. L'attribuzione e la gestione dell'Identità digitale da parte delle Istituzioni Pubbliche devono essere accompagnate da adeguate garanzie, in particolare in termini di sicurezza.

Art. 10.

(Protezione dell'anonimato).

1. Ogni persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure.

2. Limitazioni possono essere previste solo quando siano giustificate dall'esigenza di tutelare rilevanti interessi pubblici e risultino necessarie, proporzionate, fondate sulla legge e nel rispetto dei caratteri propri di una società democratica.

3. Nei casi di violazione della dignità e dei diritti fondamentali, nonché negli altri casi previsti dalla legge, l'autorità giudiziaria, con provvedimento motivato, può disporre l'identificazione dell'autore della comunicazione.

Art. 11.

(Diritto all'oblio).

1. Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica.

2. Il diritto all'oblio non può limitare la libertà di ricerca e il diritto dell'opinione pubblica a essere informata, che costituiscono condizioni necessarie per il funzionamento di una società democratica. Tale diritto può essere esercitato dalle persone note o alle quali sono affidate funzioni pubbliche solo se i dati che le riguardano non hanno alcun rilievo in relazione all'attività svolta o alle funzioni pubbliche esercitate.

3. Se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all'autorità giudiziaria per garantire l'interesse pubblico all'informazione.

Art. 12.

(Diritti e garanzie delle persone sulle piattaforme).

1. I responsabili delle piattaforme digitali sono tenuti a comportarsi con lealtà e correttezza nei confronti di utenti, fornitori e concorrenti.

2. Ogni persona ha il diritto di ricevere informazioni chiare e semplificate sul funzionamento della piattaforma, a non veder modificate in modo arbitrario le condizioni contrattuali, a non subire comportamenti che possono determinare difficoltà o discriminazioni nell'accesso. Ogni persona deve in ogni caso essere informata del mutamento delle condizioni contrattuali. In questo caso ha diritto di interrompere il rapporto, di avere copia dei dati che la riguardano in forma interoperabile, di ottenere la cancellazione dalla piattaforma dei dati che la riguardano.

3. Le piattaforme che operano in Internet, qualora si presentino come servizi essenziali per la vita e l'attività delle persone, assicurano, anche nel rispetto del principio di concorrenza, condizioni per una adeguata interoperabilità, in presenza di parità di condizioni contrattuali, delle loro principali tecnologie, funzioni e dati verso altre piattaforme.

Art. 13.

(Sicurezza in rete).

1. La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone.

2. Non sono ammesse limitazioni della libertà di manifestazione del pensiero. Deve essere garantita la tutela della dignità delle persone da abusi connessi a comportamenti quali l'incitamento all'odio, alla discriminazione e alla violenza.

Art. 14.

(Governo della rete).

1. Ogni persona ha diritto di vedere riconosciuti i propri diritti in Rete sia a livello nazionale che internazionale.

2. Internet richiede regole conformi alla sua dimensione universale e sovranazionale, volte alla piena attuazione dei principi e diritti prima indicati, per garantire il suo carattere aperto e democratico, impedire ogni forma di discriminazione e evitare che la sua disciplina dipenda dal potere esercitato da soggetti dotati di maggiore forza economica.

3. Le regole riguardanti la Rete devono tenere conto dei diversi livelli territoriali (sovranazionale, nazionale, regionale), delle opportunità offerte da forme di autoregolamentazione conformi ai principi indicati, della necessità di salvaguardare la capacità di innovazione anche attraverso la concorrenza, della molteplicità di soggetti che operano in Rete, promuovendone il coinvolgimento in forme che garantiscano la partecipazione diffusa di tutti gli interessati. Le istituzioni pubbliche adottano strumenti adeguati per garantire questa forma di partecipazione.

4. In ogni caso, l'innovazione normativa in materia di Internet è sottoposta a valutazione di impatto sull'ecosistema digitale.

5. La gestione della Rete deve assicurare il rispetto del principio di trasparenza, la responsabilità delle decisioni, l'accessibilità alle informazioni pubbliche, la rappresentanza dei soggetti interessati.

6. L'accesso e il riutilizzo dei dati generati e detenuti dal settore pubblico debbono essere garantiti.

7. La costituzione di autorità nazionali e sovranazionali è indispensabile per garantire effettivamente il rispetto dei criteri indicati, anche attraverso una valutazione di conformità delle nuove norme ai principi di questa Dichiarazione.

BIBLIOGRAFIA

Testi

ACCIAI R. *Il Diritto alla Protezione dei dati personali. La disciplina della privacy alla luce del nuovo codice,* in Acciai R. (a cura di) Maggioli Editore, Gennaio 2014, p. 29-63; 67-75; 88-91;181– 220; 92-135.

BRAVO F., *Le condizoni di leicità nel trattamento dati*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 35-38; 52-61.

CAREY P., *E-Privacy and online data protection*, Butterworths Lexis Nexis, Settembre 2002, p.

D'ACQUISTO G., NALDI M., *Big Data e Privacy by Design Anonimizzazione Pseudonimizzazione Sicurezza*, G. Giappichelli Editore (2017)

DONEDA D., ANDRADE N., VIOLA DE AZEVEDO CUNHA M., *La re-identificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, Modena: Enrico Mucchi Editore, 2010, p. 641-655

FLORIDI L., *La rivoluzione dell'Informazione*, Codici Edizioni, 2012

GORINI S., *Privacy e Comunicazioni Elettroniche*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 404-419

MAGGIOPINTO A. IASELLI M., *Sicurezza e Anonimato in rete, Profili Giuridici e Tecnologici della navigazione anonima*, Diritto ed Economia delle Nuove Tecnologie a cura di Daniele Minotti, Nyberg Edizioni, 2005 p. 47-68

MONDUCCI J., *Diritti della Persona e trattamento dei dati particolari,* Ed. Giuffrè Milano, 2003 p. 10-25.

MONDUCCI J., *Le condizoni di leicità nel trattamento dati*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 80-93.

Morelato E., *Anonimato e Protezione dei dati personali*, in Giusella Finocchiaro (a cura di), "Diritto all'anonimato, Anonimato, nome e identità personale", CEDAM, 2008, p. 12-20.

NIGER S., *Il Diritto alla protezione dei dati personali*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 1-17

NIGER S., *Privacy e Comunicazioni Elettroniche*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 387-403

NIGER S., *Le nuove dimensioni della privacy : dal diritto alla riservatezza alla protezione dei dati personali,* CEDAM, 2006, p.. 122-162

PAGALLO U., *Privacy e Design*, in M. Pietrangelo (a cura di), "Diritti di libertà nel mondo virtuale della rete", Rivista "Informatica e diritto", Vol. XVIII, 2009, n. 1, p. 123-134

PELINO E., *La nozione di anonimo*, in Giusella Finocchiaro (a cura di), "Diritto all'anonimato, Anonimato, nome e identità personale", CEDAM, 2008, p. 43-57, 289-319

PERRI P., *Le misure di sicurezza*, in Juri Monducci e Giovanni Sartor (a cura di), "Il Codice in materia di protezione dei dati personali", Commentario sistematico al D.lgs. 30 Giugno 2003 n. 196, CEDAM, 2004, p. 137-157.

PERRI P., *Privacy Diritto e Sicurezza Informatica*, Ed. Giuffrè Milano, 2007, p.. 3-25; 77-79; 85-91.

RODOTÀ S., *Il mondo nella rete. Quali i Diritti* , Editori Laterza, Marzo 2014.

RODOTÀ S., *Privacy e costruzione della sfera privata*, in Id., "Tecnologie e diritti", Bologna, Il Mulino, 1995, p.

WARREN S., BRANDEIS L., *The Right to Privacy*, in Harvard Law Review, 1890, 4, p. 193-220

Normativa Italiana e Comunitaria, pareri e linee guida

Decreto Legislativo 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Linee guida in materia di trattamento di dati personali per profilazione on line, n. 161, 19 marzo 2015. G.U. n. 103 del 60 Maggio 2015

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI , Relazione anno 2014, p. 89-92, 94-98, 99-100

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento relativo all' "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie", n. 229, 8 maggio 2014, G.U. n. 126 del 3 giugno 2014

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Linee guida in materia di trattamento di dati personali per profilazione on line - 19 marzo 2015, G.U. n. 103 del 6 maggio 2015

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., Social privacy. Come tutelarsi nell'era dei social network, 23 Maggio 2014

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati", n.243, 15 Maggio 2014, G.U. n. 134 del 12 giugno 2014

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Relazione anno 2013, La protezione dei dati nel cambiamento Big data Trasparenza Sorveglianza, p.91-101

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI Relazione anno 2012, Protezione dei dati, trasparenza e tecnologie della comunicazione, p.158- 162, 169, 171-177

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI Relazione anno 2011, La protezione dei dati, i diritti fondamentali e la dignità della persona, p.95-97,

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI Relazione anno 2010, Evoluzione tecnologica e protezione dei dati, p.108-127

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. data breach), n. 161, 4 aprile 2013, G.U. n. 97 del 4 aprile 2013

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, L. 119/34 pubblicato nella GUUE del 4.5.2016.

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, L 281/31, pubblicata nella GUUE del 23.11.1995.

Direttiva 2002/58/EC del Parlamento Europeo e del consiglio, 12 Luglio 2002 - sul trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche.

Direttiva 2009/136/CE del Parlamento Europeo e del Consiglio, 25 Novembre 2009, recante modifica delle direttive 2002/22/CE, 2002/58/CE e del Regolamento (CE) n. 2006/2004

Direttiva 2006/24/ CE del Parlamento Europeo e del Consiglio, 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito del la fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

Carta dei Diritti fondamentali dell'Unione Europea (2012/C 326/02)

COUNCIL OF EUROPE, *Data Protection Day: guidelines to protect the people behind Big Data,* 27 Gennaio 2017

Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati,* 2014

ARTICLE 29 DATA PROTECTION WORKING PARTY
WP 221, 16 September 2014, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU

WP 223, 16 September 2014, Opinion 8/2014 on the Recent Developments on the Internet of Things

WP 218, 30 May 2014, Statement on the role of a risk-based approach in data protection legal Frameworks

WP 215, 10 April 2014, Opinion 04/2014 on "Surveillance of electronic communications for intelligence and national security purposes

WP 216, 10 April 2014, Opinion 05/2014 on Anonymisation Techniques

WP 213, 25 March 2014 Opinion 03/2014 on Personal Data Breach Notification

WP 211, 14 February 2014, Opinion 01/2014 on the "Application of necessity and proportionality concepts and data protection within the law enforcement sector"

WP 208, 2 October 2013, Opinion 02/2013 providing guidance on obtaining consent for cookies

WP 202, 27 February 2013, Opinion 02/2013 on apps on smart devices

WP 199, 05 October 2012, Opinion 08/2012 providing further input on the data protection reform discussions

WP 197, 12 July 2012, Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications

WP 196, 1 July 2012, Opinion 05/2012 on Cloud Computing

WP 194, 7 June 2012, Opinion 04/2012 on Cookie Consent Exemption

WP 191, 23 March 2012, Opinion 01/2012 on the data protection reform proposals

WP 187, 13 July 2011, Opinion 15/2011 on the definition of consent

WP 184, 5 April 2011, Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments

WP 168, 01 December 2009, 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 163, 12 June 2009, Opinion 5/2009 on online social networking

WP 148, 4 April 2008, Opinion 1/2008 on data protection issues related to search engines

WP 136, 20 June 2007, Opinion 4/2007 on the concept of personal data

WP 118, 21 February 2006, Opinion 2/2006 on privacy issues related to the provision of email screening services

WP 43, 17 May 2001, Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union

Horizon 2020, Work Programme 2014 – 2015, 2016 – 2017, 14. Secure societies – Protecting freedom and security of Europe and its citizens

Banche dati e risorse elettroniche

ACQUISTI ALESSANDRO, *Privacy and Security of Personal Information: Technological Solutions and Economic Incentives*, In J. Camp and R. Lewis (eds), The Economics of Information Security, Kluwer, 165-178 (2004)

ACQUISTI ALESSANDRO, *Privacy,* Rivista di Politica Economica, V/VI, 319-368 (2005)

ACQUISTI ALESSANDRO, GROSS RALPH AND STUTZMAN FRED, *Face Recognition and Privacy in the Age ofAugmented Reality,* Journal of Privacy and Confidentiality, 6(2) (2014)

ACQUISTI ALESSANDRO, TAYLOR CURTIS R., WAGMAN LIAD, *The Economics of Privacy,* Journal of Economic Literature, forthcoming (2015)

ACQUISTI ALESSANDRO, *Identity Management, Privacy, and Price Discrimination,* Security & Privacy, Year: 2008, Volume: 6, Issue: 2 p. 46 – 50 (2008)

ALMUTAIRI ABULGADER, SIEWE FRANÇOIS, *CA-UCON: a context-aware usage control model*, Published in: Proceeding CASEMANS '11 Proceedings of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems, Pages 38-43 ACM New York, NY, USA ©2011, table of contents ISBN: 978-1-4503-0877-9 doi> 10.1145/2036146.2036153 (2011)

ARDAGNA CLAUDIO AGOSTINO, DE CAPITANI DI VIMERCATI SABRINA, SAMARATI PIERANGELA, *Privacy Models and Languages: Access Control and Data Handling Policies,* Digital Privacy, Volume 6545 of the series Lecture Notes in Computer Science, p. 309-329 (2011)

AULETTA VINCENZO, BLUNDO CARLO, DE CARO ANGELO, DE CRISTOFARO EMILIANO, PERSIANO GIUSEPPE, VISCONTI IVAN, *Increasing Privacy Threats in the Cyberspace: The Case of Italian E-Passports,* Financial Cryptography and Data Security, Volume 6054 of the series Lecture Notes in Computer Science, p. 94-104 (2010)

BAGGA WALID, MOLVA REFIK, *Policy-Based Cryptography and Applications,* Financial Cryptography and Data Security, Volume 3570 of the series Lecture Notes in Computer Science p. 72-87 (2005)

BAGÜÉS SUSANA ALCALDE, ZEIDLER ANDREAS, VALDIVIELSO CARLOS FERNANDEZ, R. MATIAS IGNACIO, *A User-Centric Privacy Framework for Pervasive Environments,* On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Volume 4278 of the series Lecture Notes in Computer Science, p. 1347-1356 (2006)

BARHAMGI MAHMOUD, BENSLIMANE DJAMAL, OULMAKHZOUNE SAID, CUPPENS-BOULAHIA NORA, CUPPENS FREDERIC, MRISSA MICHAEL, TAKTAK HAJER, *Secure and Privacy-Preserving*

Execution Model for Data Services, Advanced Information Systems Engineering, Volume 7908 of the series Lecture Notes in Computer Science, p. 35-50 (2013)

BERENDT BETTINA, *More than modelling and hiding: towards a comprehensive view of Webmining and privacy,* Data Mining and Knowledge Discovery May 2012, Volume 24 of the series Lecture Notes in Computer Science, Issue 3, p. 697-737 (2012)

BERTHOLD STEFAN, *Towards a Formal Language for Privacy Options,* Privacy and Identity Management for Life, Volume 352 of the series IFIP Advances in Information and Communication Technology, Lecture Notes in Computer Science p. 27-40 (2011)

BERTINO ELISA, BYUN JI-WON, LI NINGHUI, *Privacy-Preserving Database Systems,* Foundations of Security Analysis and Design III, Volume 3655 of the series Lecture Notes in Computer Science, p. 178-206 (2005)

BERTINO, E., *Big Data -- Opportunities and Challenges Panel Position Paper,* Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual Year: 2013, p. 479 – 480 (2013)

BEZZI MICHELE, TRABELSI SLIM, *Data Usage Control in the Future Internet Cloud,* The Future Internet, Volume 6656 of the series Lecture Notes in Computer Science, p. 223-231 (2011)

BICZÓK GERGELY, HUI CHIA PERN, *Interdependent Privacy: Let Me Share Your Data,* Financial Cryptography and Data Security, Volume 7859 of the series Lecture Notes in Computer Science, p. 338-353 (2013)

BÖTTCHER ALEXANDER, KAUER BERNHARD, HÄRTIG HERMANN, T*rusted Computing Serving an Anonymity Service,* Trusted Computing - Challenges and Applications, Volume 4968 of the series Lecture Notes in Computer Science, p. 143-154 (2008)

BRODER ALAN J., *Data Mining the Internet and Privacy,* Web Usage Analysis and User Profiling, Volume 1836 of the series Lecture Notes in Computer Science, p. 56-73 (2002)

BÜNNIG CHRISTIAN, *Smart Privacy Management in Ubiquitous Computing Environments,* Human Interface and the Management of Information, Information and Interaction, Volume 5618 of the series Lecture Notes in Computer Science, p. 131-139 (2009)

CASASSA MONT MARCO, PEARSON SIANI, *An Adaptive Privacy Management System for Data Repositories,* Trust, Privacy, and Security in Digital Business, Volume 3592 of the series Lecture Notes in Computer Science, p. 236-245 (2005)

CASASSA MONT MARCO, THYN ROBERT, *A Systemic Approach to Automate Privacy Policy Enforcement in Enterprises,* Privacy Enhancing Technologies, Volume 4258 of the series Lecture Notes in Computer Science p. 118-134 (2006)

CASASSA MONT MARCO, MATTEUCCI ILARIA, PETROCCHI MARINELLA, SBODIO MARCO LUCA, *Towards safer information sharing in the cloud,* International Journal of Information Security August 2015, Volume 14, Issue 4, p. 319-334 (2015)

CASTELLUCCIA CLAUDE, DE CRISTOFARO EMILIANO, PERITO DANIELE, *Private Information Disclosure from Web Searches,* Privacy Enhancing Technologies, Volume 6205 of the series Lecture Notes in Computer Science, p. 38-55 (2010)

CAVOUKIAN ANN, *Privacy in the clouds,* Identity in the Information Society, December 2008, Volume 1, Issue 1, p. 89-108 (2008)

CAVOUKIAN ANN, *Privacy by Design, The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (2013)

CAVOUKIAN ANN, *Privacy by Design and the Emerging Personal Data Ecosystem* (2012)

CAVOUKIAN ANN, REED DRUMMOND, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem Through Privacy by Design* (2013)

CHADWICK D.W., LIEVENS S.F., HARTOG DEN J. I., PASHALIDIS A., ALHADEFF J., *My Private Cloud Overview: A Trust, Privacy and Security Infrastructure for the Cloud,* Cloud Computing (CLOUD), 2011 IEEE International Conference on Year: 2011, p. 752 – 753

CHADWICK DAVID W., FATEMA KANIZ, *An advanced policy based authorisation infrastructure*, DIM '09: Proceedings of the 5th ACM workshop on Digital Identity Management (2009)

CHADWICK DAVID W., LIEVENS STIJN F., *Enforcing "Sticky" security policies throughout a distributed application,* MidSec '08: Proceedings of the 2008 workshop on Middleware security (2008)

CHEN MIN, MAO SHIWEN, LIU YUNHAO, *Big Data: A Survey,* Mobile Networks and Applications, April 2014, Volume 19, Issue 2, p. 171-209 (2014)

CORTESI AGOSTINO, FERRARA PIETRO, PISTOIA MARCO, TRIPP OMER, *Datacentric Semantics for Verification of Privacy Policy Compliance by Mobile Applications,* Verification, Model Checking, and Abstract Interpretation, Volume 8931 of the series Lecture Notes in Computer Science, p. 61-79 (2015)

CORTIS KEITH, SCERRI SIMON, RIVERA ISMAEL, *Techniques for the Identification of Semantically-Equivalent Online Identities,* Resource Discovery, Volume 8194 of the series Lecture Notes in Computer Science p. 1-22 (2013)

CREESE SADIE, HOPKINS PAUL, PEARSON SIANI, SHEN YUN, *Data Protection-Aware Design for Cloud Services,* Cloud Computing, Volume 5931 of the series Lecture Notes in Computer Science, p. 119-130 (2009)

CUTILLO L.A., MOLVA R., STRUFE T., *Privacy preserving social networking through decentralization,* Wireless On-Demand Network Systems and Services, 2009, WONS 2009, Sixth International Conference on Year: 2009, p. 145 – 15 (2009)

DE ANGELIS GUGLIELMO, KIRKHAM TOM, WINFIELD SANDRA, *Access policy compliance testing in a user centric trust service infrastructure,* QASBA '11: Proceedings of the International Workshop on Quality Assurance for Service-Based Applications (2011)

De Capitani di Vimercati Sabrina, Foresti Sara, Livraga Giovanni, Samarati Pierangela, *Protecting Privacy in Data Release,* Foundations of Security Analysis and Design VI, Volume 6858 of the series Lecture Notes in Computer Science p. 1-34 (2011)

De Hert P., Gutwirth S., Moscibroda A., Wright D., Gonzalez Fuster G., *Legal safeguards for privacy and data protection in ambient intelligence*, Springer-Verlag London Limited (2008)

De Masellis Riccardo, Ghidini Chiara, Ranise Silvio, *A Declarative Framework for Specifying and Enforcing Purpose-Aware Policies,* Security and Trust Management, Volume 9331 of the series Lecture Notes in Computer Science p. 55-71 (2015)

De Montjoye Yves-Alexandre, Hidalgo César A., Verleysen Michel, Blondel Vincent D., "*Unique in the Crowd: The privacy bounds of human mobility,*" Nature, Scientific Reports 3, Article number: 1376 (2013), doi:10.1038/srep01376, http://www.nature.com/articles/srep01376 (2013) Last Accessed:

Demchenko Yuri, Ngo Canh, de Laat Cees, Membrey Peter, Gordijenko Daniil, *Big Security for Big Data: Addressing Security Challenges for the Big Data Infrastructure,* Secure Data Management, Volume 8425 of the series Lecture Notes in Computer Science p. 76-94 (2014)

De Vries W. T., *Protecting Privacy in the Digital Age,* Berkeley Technology Law Journal Volume 18, Issue 1 Article 19, January 2003 (2003)

Dhami A., Agarwal N., Chakraborty T.K., Singh B.P., Minj J., *Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook,* Advance Computing Conference (IACC), 2013 IEEE 3rd International Year: 2013, p. 465 – 469 (2013)

Di Cerbo Francesco, Trabelsi Slim, Steingruber Thomas, Dodero Gabriella, Bezzi Michele, *Sticky policies for mobile devices,* SACMAT '13: Proceedings of the 18th ACM symposium on Access control models and technologies (2013)

Doyle Tony, Veranas Judy, *Public anonymity and the connected world,* Ethics and Information Technology September 2014, Volume 16, Issue 3, p. 207-218 (2014)

Dua Akshay, Bulusu Nirupama, Feng Wu-chang, *Privacy-Preserving Online Mixing of High Integrity Mobile Multi-user Data,* Security and Privacy in Communication Networks, Volume 96 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, p. 470-479

Eldin A.A., Wagenaar R., *Towards users driven privacy control,* Systems, Man and Cybernetics, 2004 IEEE International Conference on Year: 2004, Volume: 5, p. 4673 - 4679 vol.5 (2004)

Eldin A.A., Wagenaar R., *A Privacy Preferences Architecture for Context Aware Applications,* Computer Systems and Applications, 2006, IEEE International Conference on. Year: 2006, p. 1110 – 1113 (2006)

Ensen M., *Challenges of Privacy Protection in Big Data Analytics,* Big Data (BigData Congress) 2013, IEEE International Congress on Year: 2013, p. 235 – 238 (2013)

FARAVELON A., CHOLLET S., VERDIER C., FRONT A., *Enforcing privacy as access control in a pervasive context,* Consumer Communications and Networking Conference (CCNC), 2012 IEEE Year: 2012, p. 380 - 384 (2012)

FATEMA KANIZ, CHADWICK DAVID W., LIEVENS STIJN, *A Multi-privacy Policy Enforcement System,* Privacy and Identity Management for Life, Volume 352 of the series IFIP Advances in Information and Communication Technology, p. 297-310 (2011)

FINNERAN DENNEDY MICHELLE, FOX JONATHAN, FINNERAN THOMAS R., *Value and Metrics for Data Assets,* The Privacy Engineer's Manifesto, p. 279-298 2014)

FINNERAN DENNEDY MICHELLE, FOX JONATHAN, FINNERAN THOMAS R., *Technology Evolution, People, and Privacy,* The Privacy Engineer's Manifesto, p. 3-24 (2014)

FINNERAN DENNEDY MICHELLE, FOX JONATHAN, FINNERAN THOMAS R., *Developing Privacy Engineering Requirements,* The Privacy Engineer's Manifesto, p. 93-120 (2014)

FINNERAN DENNEDY MICHELLE, FOX JONATHAN, FINNERAN THOMAS R., *A Privacy Engineering Lifecycle Methodology,* The Privacy Engineer's Manifesto, p. 121-160 (2014)

FLORIDI LUCIANO, *On Human Dignity as a Foundation for the Right to Privacy*, Philos. Technol. DOI 10.1007/s13347-016-0220-8, Springer Science+Business Media Dordrecht 2016

FLORIDI LUCIANO, *The ontological interpretation of informational privacy. Ethics and Information Technology,* p.185–200.

FLORIDI LUCIANO, *Four challenges for a theory of informational privacy. Ethics and Information Technology,* p. 109–119.

FINNERAN DENNEDY MICHELLE, FOX JONATHAN, FINNERAN THOMAS R., *Developing Privacy Policies,* The Privacy Engineer's Manifesto, p. 75-92 (2014)

GAO JERRY, LI SHUYU, ZHANG TAO, *A Sticky Policy Framework for Big Data Security*, Sponsored by China Scholarship Council,
https://www.researchgate.net/publication/273635349, CONFERENCE PAPER · MARCH 2015 (2015)

GARCIA-BARRIOS V.M., *User-centric Privacy Framework: Integrating Legal, Technological and Human Aspects into User-Adapting Systems,* Computational Science and Engineering, 2009. CSE '09. International Conference on Year: 2009, Volume: 3, p.176 - 181 (2009)

GEHRKE JOHANNES, HAY MICHAEL, LUI EDWARD, PASS RAFAEL, *Crowd-Blending Privacy,* Advances in Cryptology – CRYPTO 2012, Volume 7417 of the series Lecture Notes in Computer, Science p. 479-496 (2012)

GHANI IMRAN, LEE CHOON YEUL, JUHN SUNG HYUN, JEONG SEUNG RYUL, *Semantics-oriented approach for information interoperability and governance: towards user-centric enterprise architecture*

management, Journal of Zhejiang University SCIENCE C, April 2010, Volume 11, Issue 4, p. 227-240 (2010)

GLISSON WILLIAM BRADLEY, STORER TIM, MAYALL GAVIN, MOUG IAIN, GRISPOS GEORGE, *Electronic retention: what does your mobile phone reveal about you?,* International Journal of Information Security, November 2011, Volume 10, Issue 6, p. 337-349 (2011)

GNESI STEFANIA, MATTEUCCI ILARIA, MOISO CORRADO, MORI PAOLO, PETROCCHI MARINELLA, VESCOVI MICHELE, *My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data,* Privacy Technologies and Policy, Volume 8450 of the series Lecture Notes in Computer Science p. 154-171 (2014)

GONZÁLEZ-MANZANO LORENA, BROST GERD, AUMUELLER MATTHIAS, *An Architecture for Trusted PaaS Cloud Computing for Personal Data,* Trusted Cloud Computing, p. 239-258,(2014)

GÜRSES SEDA, *PETs and their users: a critical review of the potentials and limitations of the privacy as confidentiality paradigm,* Identity in the Information Society, December 2010, Volume 3, Issue 3, p. 539-563 (2010)

HENRICKSEN K., WISHART R., MCFADDEN T., INDULSKA J., *Extending context models for privacy in pervasive computing environments,* Pervasive Computing and Communications Workshops, 2005, PerCom 2005 Workshops. Third IEEE International Conference on Year: 2005, p. 20 – 24 (2005)

HOEPMAN JAAP-HENK, *Privacy Design Strategies, (Extended Abstract),* ICT Systems Security and Privacy Protection, Volume 428 of the series IFIP Advances in Information and Communication Technology, p. 446-459 (2012)

HOFFMANN MARIO, *An App Approach Towards User Empowerment in Personalized Service Environments,* Service-Oriented and Cloud Computing, Volume 8135 of the series Lecture Notes in Computer Science, p. 149-163 (2013)

HUBER MATTHIAS, MÜLLER-QUADE JÖRN, NILGES TOBIAS, *Defining Privacy Based on Distributions of Privacy Breaches,* Number Theory and Cryptography, Volume 8260 of the series Lecture Notes in Computer Science, p. 211-225 (2013)

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*, 15 Dicembre 2011 (First Edition) (2011)

JONES SIMON, HARA SUKHVINDER, AUGUSTO JUAN CARLOS, *eFRIEND: an ethical framework for intelligent environments development,* Ethics and Information Technology, March 2015, Volume 17, Issue 1, p. 11-25 (2015)

KAISLER S., ARMOUR F., ESPINOSA J.A., MONEY W., *Big Data: Issues and Challenges Moving Forward,* System Sciences (HICSS), 2013 46th Hawaii International Conference on Year: 2013, p. 995 – 1004 (2013)

KAISLER STEPHEN, ARMOUR FRANK, ESPINOSA J.ALBERT, *Introduction to Big Data: Challenges, Opportunities, and Realities,* System Sciences (HICSS), 2014 47th Hawaii International Conference on Year: 2014, p. 728 – 728 (2014)

KELBERT FLORIAN, PRETSCHNER ALEXANDER, *Towards a policy enforcement infrastructure for distributed usage control*, SACMAT '12: Proceedings of the 17th ACM symposium on Access Control Models and Technologies (2012)

KELBERT FLORIAN, PRETSCHNER ALEXANDER, *Data usage control enforcement in distributed systems*, Proceeding CODASPY '13 Proceedings of the third ACM conference on Data and application security and privacy, Pages 71-82, ACM New York, NY, USA ©2013 table of contents ISBN: 978-1-4503-1890-7 doi>10.1145/2435349.243535 (2013)

KIRKHAM T., WINFIELD S., RAVET S., KELLOMAKI S., *The Personal Data Store Approach to Personal Data Security,* Security & Privacy, IEEE Year: 2013, Volume: 11, Issue: 5, p. 12 – 19 (2013)

KIRKHAM T., WINFIELD S., RAVET S., KELLOMAKI S., *A personal data store for an Internet of Subjects,* Information Society (i-Society), 2011 International Conference on Year: 2011, p. 92 – 97, IEEE Conference Publications (2011)

KLITOU DEMETRIUS, *Privacy, Liberty and Security,* Privacy-Invading Technologies and Privacy by Design, Volume 25 of the series Information Technology and Law Series, p. 13-25 (2014)

KOLTER JAN, KERNCHEN THOMAS, PERNUL GÜNTHER, *Collaborative Privacy – A Community-Based Privacy Infrastructure,* Emerging Challenges for Security, Privacy and Trust, Volume 297 of the series IFIP Advances in Information and Communication Technology, p. 226-236 (2009)

KOLTER J., PERNUL G., *Generating User-Understandable Privacy Preferences,* Availability, Reliability and Security, 2009, ARES '09, International Conference on Year: 2009, p. 299 – 306

KONINGS B., SCHAUB F., WEBER M., *Who, how, and why? Enhancing privacy awareness in Ubiquitous Computing,* Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on Year: 2013, p. 364 - 367 (2013)

KOUNGA GINA, CASASSA MONT MARCO, BRAMHALL PETE, *Extending XACML Access Control Architecture for Allowing Preference-Based Authorisation,* Trust, Privacy and Security in Digital Businessm, Volume 6264 of the series Lecture Notes in Computer Science, p. 153-164 (2010)

KUNG ANTONIO, *ICT and Privacy: Barriers,* Privacy Technologies and Policy, Volume 8319 of the series Lecture Notes in Computer Science, p. 177-186 (2014)

LÄMMEL RALF, PEK EKATERINA, *Understanding privacy policies A study in empirical analysis of language usage,* Empirical Software Engineering, April 2013, Volume 18, Issue 2, p. 310-374 (2012)

LANGHEINRICH MARC, *A Privacy Awareness System for Ubiquitous Computing Environments,* UbiComp 2002: Ubiquitous Computing, Volume 2498 of the series Lecture Notes in Computer Science, p. 237-245 (2002)

LANGHEINRICH MARC, *Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems,* Ubicomp 2001: Ubiquitous Computing Volume 2201 of the series Lecture Notes in Computer Science, p. 273-291 (2001)

LEDERER S., MANKOFF J., DEY ANIND. K., BECKMANN CHRISTOPHER P., *Managing Personal Information Disclosure in Ubiquitous Computing Environments,* Report No. UCB/CSD-3-1257, July 2003, Computer Science Division (EECS), University of California (2003)

MAGAGNA F., JACCOMUTHU M., SUTANTO *J., CA2P: An Approach for Privacy-Safe Context-Aware Services for Mobile Phones,* Ubi-Media Computing (U-Media), 2011 4th International Conference on Year: 2011, p. 89 - 94 (2011)

MIN MUN, SHUAI HAO, NILESH MISHRA, KATIE SHILTON, JEFF BURKE, DEBORAH ESTRIN, MARK HANSEN, RAMESH GOVINDAN, *Personal data vaults: a locus of control for personal data streams,* Co-NEXT '10: Proceedings of the 6th International Conference (2010)

MONT CASASSA M., PEARSON S., BRAMHALL, P., *Towards accountable management of identity and privacy: sticky policies and enforceable tracing services,* Database and Expert Systems Applications, 2003, Proceedings. 14th International Workshop on Year: 2003, p. 377 – 382 (2003)

MONT CASASSA, M., PEARSON S., BRAMHALL, P., *Towards Accountable Management of Privacy and Identity Information,* Computer Security – ESORICS 2003, Volume 2808 of the series Lecture Notes in Computer Science, p. 146-161 (2003)

NARAYANAN ARVIND, SHMATIKOV VITALY, *De-anonymizing Social Networks*, 30th IEEE Symposium on Security and Privacy, Year: 2009 Pages: 173 - 187, DOI: 10.1109/SP.2009.22 (2009)

NAVARRO-ARRIBAS GUILLERMO, ABRIL DANIEL, TORRA VICENÇ, *Dynamic Anonymous Index for Confidential Data,* Data Privacy Management and Autonomous Spontaneous Security, Volume 8247 of the series Lecture Notes in Computer Science, p. 362-368 (2014)

NIEMI, V., *Privacy, Identity and Trust in Context-Aware Mobile Services,* Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on Year: 2011, p. 9 – 10 (2011)

NUÑEZ DAVID, AGUDO ISAAC, LOPEZ JAVIER, *Privacy-Preserving Identity Management as a Service,* Accountability and Security in the Cloud, Volume 8937 of the series Lecture Notes in Computer Science, p. 114-125 (2015)

NUNO NORBERTO, DE ANDRADE GOMES, *Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights,* Privacy and Identity Management for Life, Volume 352 of the series IFIP Advances in Information and Communication Technology p. 90-107 (2011)

O'DRISCOLL, C., *Privacy in context: Privacy issues in Ubiquitous Computing applications,* Digital Information Management, 2008, ICDIM 2008, Third International Conference on Year: 2008, p. 827 - 837 (2008)

PEARSON SIANI, *On the Relationship between the Different Methods to Address Privacy Issues in the Cloud* On the Move to Meaningful Internet Systems: OTM 2013 Conference, Volume 8185 of the series Lecture Notes in Computer Science, p. 414-433 (2013)

PEARSON S., MONT CASASSA M., *Sticky Policies: An Approach for Managing Privacy across Multiple Parties,* Computer Year: 2011, Volume: 44, Issue: 9, p. 60 – 68 (2011)

PRETSCHNER ALEXANDER, HILTY MANUEL, BASIN DAVID, *Distributed Usage Control*, Magazine Communications of the ACM - Privacy and security in highly dynamic systems CACM Homepage archive, Volume 49 Issue 9, September 2006, Pages 39-44 (2006)

PRETSCHNER A., HILTY M., BASIN D., SCHAEFER C., WALTER T., *Mechanisms for usage control*, Published by ACM 2008 Article, Published in: Proceeding ASIACCS '08 Proceedings of the 2008 ACM symposium on Information, computer and communications security, pages 240-244, ACM New York, NY, USA ©2008, table of contents ISBN: 978-1-59593-979-1 doi>10.1145/1368310.1368344 (2008)

QINGSHENG ZHANG, YONG QI, JIZHONG ZHAO, DI HOU, TIANHAI ZHAO, JIHONG ZHANG, *Context-Aware Learning Privacy Disclosure Policy from Interaction History*, Natural Computation, 2007, ICNC 2007, Third International Conference on Year: 2007, Volume: 5, p. 3 - 7 (2007)

QINGSHENG ZHANG, YONG QI, JIZHONG ZHAO, DI HOU; TIANHAI ZHAO, LIANG LIU, *A Study on Context-aware Privacy Protection for Personal Information,* Computer Communications and Networks, 2007, ICCCN 2007, Proceedings of 16th International Conference on Year: 2007, p. 1351 - 1358 (2007)

RANE D.D., GHORPADE V.R., *Multi-user multi-keyword privacy preserving ranked based search over encrypted cloud data,* Pervasive Computing (ICPC), 2015 International Conference on Year: 2015, p. 1 – 4 (2015)

ROMANOSKY SASHA AND ACQUISTI ALESSANDRO, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives,* Berkeley Technology Law Journal, 24(3), 1061-1102 (2009)

SCHAAR PETER, *Privacy by Design,* Identity in the Information Society, August 2010, Volume 3, Issue 2, p. 267-274 (2010)

SCHRECKLING DANIEL, POSEGGA JOACHIM, HAUSKNECHT DANIEL, *Constroid: data-centric access control for android*, Proceeding SAC '12 Proceedings of the 27th Annual ACM Symposium on Applied Computing, Pages 1478-1485, ACM New York, NY, USA ©2012, table of contents ISBN: 978-1-4503-0857-1 doi>10.1145/2245276.2232012 (2012)

SCHEFFLER THOMAS, GEISS STEFAN, SCHNOR BETTINA, *An Implementation of a Privacy Enforcement Scheme based on the Java Security Framework using XACML Policies*, Proceedings of The Ifip Tc 11 23rd International Information Security Conference, Volume 278 of the series IFIP – The International Federation for Information Processing, p. 157-171 (2008)

SCHIERING INA, KRETSCHMER JAN, *The Infrastructure Level of Cloud Computing as a Basis for Privacy and Security of Software Services,* Privacy and Identity Management for Life, Volume 375 of the series IFIP Advances in Information and Communication Technology, p. 88-101

SHORT STUART, KALUVURI SAMUEL PAUL, *A Data-Centric Approach for Privacy-Aware Business Process Enablement,* Enterprise Interoperability, Volume 76 of the series Lecture Notes in Business Information Processing, p. 191-203 (2011)

SHUAI HUIMIN, TAO ZHU WEN, *Masque: Access Control for Interactive Sharing of Encrypted Data in Social Networks,* Network and System Security, Volume 7645 of the series Lecture Notes in Computer Science, p. 503-515 (2012)

SMITH M., SZONGOTT C., HENNE B., VON VOIGT G., *Big data privacy issues in public social media,* Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on Year: 2012, p. 1 – 6 (2012)

SOMMER DIETER, *Architecture,* Digital Privacy, Volume 6545 of the series Lecture Notes in Computer Science, p. 151-288 (2011)

SPIEKERMANN SARAH, ACQUISTI ALESSANDRO, BÖHME RAINER, HUI KAI-LUNG, *The challenges of personal data markets and privacy*, Position Paper, Electronic Markets, June 2015, Volume 25, Issue 2, pp 161-167, 29 April 2015 (2015)

SQUICCIARINI ANNA C., SHEHAB MOHAMED, WEDE JOSHUA, *Privacy policies for shared content in social network sites,* The VLDB Journal, December 2010, Volume 19, Issue 6, p. 777-796 (2010)

SQUICCIARINI ANNA CINZIA, SHEHAB MOHAMED, PACI FEDERICA, *Collective privacy management in social networks,* WWW '09: Proceedings of the 18th international conference on World wide web (2009)

TOCH ERAN, *Crowdsourcing privacy preferences in context-aware applications,* Personal and Ubiquitous Computing, January 2014, Volume 18, Issue 1, p. 129-141 (2012)

TOMKO GEORGE, *SmartData: The Need, the Goal and the Challenge,* SmartData, p. 11-25 (2013)

TRABELSI S., SENDOR J., *Sticky policies for data control in the cloud,* Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on Year: 2012, p. 75 – 80 (2012)

VAN KLEEK MAX, OHARA KIERON, *The Future of Social Is Personal: The Potential of the Personal Data Store,* Social Collective Intelligence, Part of the series Computational Social Sciences p. 125-158 (2014)

VELEV DIMITER, ZLATEVA PLAMENA, *Cloud Infrastructure Security,* Open Research Problems in Network Security, Volume 6555 of the series Lecture Notes in Computer Science, p. 140-148 (2011)

VESCOVI MICHELE, MOISO CORRADO, PASOLLI MATTIA, CORDIN LORENZO, ANTONELLI FABRIZIO, *Building an Eco-System of Trusted Services via User Control and Transparency on Personal Data,* Trust Management IX, Volume 454 of the series IFIP Advances in Information and Communication Technology p. 240-250 (2015)

VESCOVI MICHELE, PERENTIS CHRISTOS, LEONARDI CHIARA, LEPRI BRUNO, MOISO CORRADO, *My data store: toward user awareness and control on personal data,* UbiComp '14 Adjunct: Proceedings

of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (2014)

VOIGTMANN C., DAVID K., SKISTIMS H., ROSSNAGEL A., *Legal assessment of context prediction techniques,* Vehicular Technology Conference (VTC Fall), 2012 IEEE Year: 2012, p. 1 - 5 (2012)

WANG HUI (WENDY), LIU RUILIN, *Hiding outliers into crowd: Privacy-preserving data publishing with outliers,* Data & Knowledge Engineering, (2015)

WOHLGEMUTH SVEN, *Adaptive User-Centered Security,* Availability, Reliability, and Security in Information Systems, Volume 8708 of the series Lecture Notes in Computer Science, p. 94-109 (2014)

WORLD ECONOMIC FORUM, *Unlocking the Value of Personal Data: From Collection to Usage,* http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage (2013), ultima consultazione: 27 Marzo 2017

WORLD ECONOMIC FORUM, *Rethinking Personal Data: A New Lens for Strengthening Trust,* http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf (2014), ultima consultazione: 27 Marzo 2017

WORLD ECONOMIC FORUM, *Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems,* http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (2014),ultima consultazione: 27 Marzo 2017

WORLD ECONOMIC FORUM, *Rethinking Personal Data: Strengthening Trust,* http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf (2012), ultima consultazione: 27 Marzo 2017

XIAODONG JIANG, LANDAY J.A., *Modeling privacy control in context-aware systems,* Pervasive Computing, IEEE Year: 2002, Volume: 1, Issue: 3, p. 59 - 63 (2002)

XINDONG WU, XINGQUAN ZHU, GONG-QING WU, WEI DING, *Data mining with big data,* Knowledge and Data Engineering, IEEE Transactions on Year: 2014, Volume: 26, Issue: 1, p. 97 - 107 (2014)

ZENO-ZENCOVICH V., *Anonymous speech on the Internet* http://www.giur.uniroma3.it/materiale/docenti/zeno/materiale/Anonymous%20speech%20(%20in%20Koltay%20ed.).pdf

ZHANG QINGSHENG, QI YONG, ZHAO JIZHONG, HOU DI, NIU YUJIE, *Research on context-aware architecture for personal information privacy protection,* Systems, Man and Cybernetics, 2007, ISIC, IEEE International Conference on Year: 2007, p. 3912 - 3916 (2007)

119 ZHANG, NI, TODD CHRIS, *A privacy-respecting context-aware architecture,* Wireless, Mobile and Multimedia Networks, 2006, IET International Conference on Year: 2006, p. 1 - 4 (2006)

ZHI-HUA ZHOU, CHAWLA N.V., YAOCHU JIN, WILLIAMS G.J., *Big Data Opportunities and Challenges: Discussions from Data Analytics Perspectives,* Computational Intelligence Magazine, IEEE Year: 2014, Volume: 9, Issue: 4 p. 62 – 74 (2014)

ZIMMERMANN CHRISTIAN, NOLTE CLAUS-GEORG, *Towards Balancing Privacy and Efficiency: A Principal-Agent Model of Data-Centric Business,* Security and Trust Management, Volume 9331 of the series Lecture Notes in Computer Science, p. 89-104 (2015)

13° Rapporto Censis-Ucsi sulla Comunicazione, *I media tra élite e popolo*, Francoangeli Editore (2016)

12° Rapporto Censis-Ucsi sulla Comunicazione, *L'economia della disintermediazione digitale*, Francoangeli Editore (2015)

10° Rapporto Censis-UCsi sulla Comunicazione, *I Media siamo noi, inizio dell'era biomediatica*, Francoangeli Editore (2012)

CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, *Rapporto CLUSIT 2015 sulla sicurezza ICT in Italia*, https://www.clusit.it/download/index.htm
Ultima consultazione: 17 Aprile 2017

CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, *Rapporto CLUSIT 2016 sulla sicurezza ICT in Italia*, https://www.clusit.it/download/index.htm
Ultima consultazione: 17 Aprile 2017