Il dato e il GDPR

Prof. Avv. Giovanni Ziccardi
Università degli Studi di Milano
Information Society Law Center
Roma, 19 gennaio 2018 - FIIF

1. PREMESSE

La “natura” del GDPR

Al centro del Regolamento vi è:

1. La **persona**: l’interessato.

Ma la persona, e i suoi diritti di libertà, si proteggono attraverso la protezione dei suoi **dati.**

È un dato che **cambia** grazie alla società dell’informazione e dei social network.

Come è il dato oggi?

1. **Preciso** (in alcuni casi: addirittura **predittivo**).
2. **Correlato o facilmente correlabile**: in un mondo fatto di *big data*.
3. Capace di **profilare**, anche in maniera automatizzata e "intelligente".
4. Mobile: che rende il **tracking** dell'informazione complesso (si pensi al cloud e allo **spostamento** costante di informazioni anche in base alle esigenze/risorse del sistema).

Da Orwell a Kafka

Cambia la tipologia di controllo del dato:

- Sistema **orwelliano**: un controllo dal **centro**, che "vede"
- Sistema **kafkiano**: un controllo **labirintico**, basato sulla burocrazia, sulla perdita di controllo, sui "muri di gomma", sui trasferimenti all'estero, sulla mancanza di riferimenti chiari (di qui l'**importanza** dell'informativa).

I dati nella tradizione della privacy:

- Anonimi.
- Personali.
- Sensibili.
- “Ultrasensibili” o particolari (era una categoria **non** formalizzata; ora lo è) .
- Pseudonimizzati.

Grande differenza tra dati in **chiaro** e dati **cifrati**, che sta caratterizzando tutta la società dell’informazione (anche) in un’ottica di **sicurezza**.

L’emergenza dei data breach

Il dato **fugge**, **esce**, e non possiamo farci nulla.

Anche la miglior sicurezza nostra, personale, non può far nulla contro un attacco al “**centro**”, ai luoghi dove i nostri dati sono custoditi (senso di impotenza…)

Tutti hanno subito o prima o poi subiranno un data breach.

Apre problemi enormi: è stato “anticipato” nel settore **pubblico**, prospetta rischi di **autodenuncia**, impatta sul rapporto coi clienti e intacca gli interessi del **business**

Un DPO (Data Protection Officer)!

Un “ufficiale”, un agente per la **protezione del dato.**

Testimonia il valore **centrale** dell’informazione.

i) Guarda all’interno, ii) guarda agli interessati, e iii) guarda all’autorità di controllo: nelle **tre direzioni** dove può sorgere un problema al dato.

L’esigenza di una **portabilità** dei dati

È spesso citata dal Garante come un punto essenziale e innovativo.

Impone un ripensamento dei sistemi che trattano i dati oggi, e prende la forma di una **trasportabilità** delle informazioni proprio come il numero di telefono.

Trattamento dati dei minori

Non solo **consenso parentale**, ma anche informativa *ad hoc* comprensibile a loro.

<u>Cosa comporta?</u>

- Riconfigurazione delle piattaforme.
- Certezza nel consenso.
- Attenzione al **linguaggio** utilizzato.

“Diritto all’oblio”

Diritto alla **cancellazione**, non all’oblio.

Come si possono rincorrere i dati (*tracking*)?

Avvertire **tutte le parti** che ricevono quei dati legittimamente che gli stessi vanno cancellati.

Dati delle persone decedute, e gestione dell’eredità digitale.

L’emendamento Kafka

Il trattamento **automatizzato** dei dati

Conseguenze giuridiche che nascono **senza** l’intervento di un essere umano.

Possibilità di opporsi, o di domandare un successivo controllo.

Paura per la **profilazione** automatica.

2. IL GDPR E IL DATO

Dato personale

Qualsiasi informazione riguardante una persona fisica **identificata** o **identificabile**.

In altri termini: qualsiasi informazione che riguardi un **interessato**.

Nozione “storica” di dato

Nozione di **dato personale** già prevista dalla Convenzione 108/**1981**.

Dati a carattere personale: “ogni informazione concernente una persona fisica identificata o identificabile”.

Definizione ripresa dalla Direttiva 95/46 e, poi, dal Regolamento.

Opinion 4/2007

Opinion 4/2007 del **Working Party** ex art. 29: è uno dei documenti di riferimento.

Soprattutto sulla nozione di identificazione/ identificabilità e sulla natura del **dato personale**.

Dato personale

Qualsiasi informazione riguardante una persona fisica **almeno** identificabile (Bolognini, Giuffrè, 2016).

I 4 elementi

Quattro elementi (Bolognini, Giuffrè, 2016):

i) **informazione** (ossia il contenuto del dato),

ii) **persona fisica** (il soggetto a cui il contenuto viene collegato),

iii) **collegamento** (operazione logica),

iv) **identificazione/identificabilità** (un attributo necessario della persona fisica, non un astratto collegamento: la persona deve essere **singolarmente** individuata o individuabile).

Informazione

Rappresentazione di cose, fatti, persone.

Qualsiasi: è indipendente dal formato di codifica (termine linguistico, formato audio, simbolo grafico, immagine fissa o in movimento, un suono, un fotogramma o altro). (Bolognini, Giuffrè, 2016)

Informazione #2

Lo è anche l'informazione irrilevante, positiva, minima o la **meta-informazione**, ossia l'informazione sulla informazione (Bolognini, Giuffrè, 2016).

Vera o falsa?

Non importa se sia vera o falsa.

Una informazione **falsa** o **imprecisa** può produrre effetti ancora più **gravi** di una informazione veritiera (Bolognini, Giuffrè, 2016).

Collegamento alla persona

Deve riguardare una persona fisica.

Sono tutte nozioni molto **astratte** e **flessibili**.

Ciò comporta che la definizione di dato personale sia **molto ampia** sul piano applicativo

identificabilità

“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”. (Art. 4)

Considerando 26

È auspicabile applicare i principi di protezione dei dati a **tutte** le informazioni relative a una persona fisica identificata o identificabile.

Considerando 26

I dati personali sottoposti a **pseudonimizzazione**, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile.

Considerando 26

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.

Considerando 26

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.

Considerando 26

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.

Considerando 26

Il regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità **statistiche** o di **ricerca**.

3 “famiglie” (Bolognini, Giuffrè)

- **Identificativo**: una informazione idonea a rendere identificata/identificabile la persona fisica.
- **Identificazione**: individuazione/riconoscimento della persona fisica anche a prescindere dal nome, diretta o indiretta.
- **Identificabilità**: è la possibilità di pervenire all’identificazione dell’interessato, valutando gli strumenti di identificazione che è ragionevolmente probabile che il titolare o un terzo utilizzino.

Rapporto con l’anonimato

- L’identificabilità è quella che fa **scattare** o meno l’anonimato.
- L’informazione anonima o anonimizzata manca di un **soggetto determinato** cui riferire il contenuto informativo.
- Due esempi più comuni di un’informazione che permette un’immediata identificazione: il **nome** o **l’immagine**.

Irrilevanza del nome anagrafico

- Ai fini della identificazione non è necessaria la determinazione del **nome anagrafico** della persona fisica ma è **sufficiente** l'individuazione della persona all'interno di un contesto, a prescindere quindi dalla conoscenza del nome.

Individuazione e riconoscimento.

Attitudine distintiva (Bolognini, Giuffrè, 2016)

Basta che il dato abbia **attitudine distintiva**.

Non rileva che la persona fisica sia individuabile da chiunque, ma ciò che conta è che possa essere distinta o riconosciuta con una ragionevole probabilità **almeno da qualcuno**, ad esempio una cerchia di persone.

Insieme di informazioni

- Una **singola informazione** può non avere sufficiente valore identificativo, ma l'attitudine a distinguere l'interessato entro un contesto può risultare dalla combinazione di più informazioni.
- Sono **insiemi di informazioni** con valore identificativo (Bolognini, Giuffrè).

Diretto o indiretto

Identificazione diretta o indiretta

- Significa un collegamento immediato o mediato dell'indentificativo rispetto alla persona fisica.
- Nome anagrafico, immagine, voce: **diretto**
- Telefono, targa, codice fiscale, ubicazione, pseudonimo, credenziali online: **indiretto**.
- È solo un criterio di massima (si pensi alla targa conosciuta a memoria da un familiare).

Ragionevole probabilità

Non qualsiasi possibile identificazione ha pregio, ma solo l'identificazione a cui si possa pervenire tenendo conto dei mezzi che è **ragionevolmente** probabile che verranno utilizzati da un titolare o da un terzo. (Bolognini, Giuffrè)

Ragionevole probabilità #2

Si parla di ragionevole probabilità che sia fatto uso di strumenti per l'identificazione dell'interessato, ossia riguarda l'aspetto **strumentale** attraverso il qual si può raggiungere alla identificazione (Bolognini, Giuffrè).

Strumenti disponibili

Attenzione agli strumenti **concretamente** disponibili nel caso di specie.

Processi deduttivi attraverso i quali è possibile approdare alla identificazione

Vi sono poi dei parametri oggettivi previsti ex lege.

Introdotti dal Gruppo di Lavoro:

1) costi, e 2) Tempo necessario.

Costo e tempo

Vanno considerati **entrambi**

- Uso di strumenti statistici, o di strumenti crittografici.
- L'attenzione e la valutazione va fatta sia *ex ante*, quanto si stabilisce la protezione, sia *ex post*, quando già sono state disposte le misure di sicurezza.

Dati pluripersonali

Un dato collegato **a più soggetti** e che quindi presenta una pluralità di interessati.

- Se si esercita il diritto di **accesso** da parte di un soggetto? Dipende se si possono separare o se viene snaturato il contenuto perché intrecciati e la separazione rende incomprensibili, allora si può comunicare. (Bolognini, Giuffrè)

I dati genetici sono **intersecamente** pluripersonali.

Dati sensibili

“È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.”

Dati genetici

«**Dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati biometrici

«**Dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute

«**Dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dati comuni vs. sensibili

Aggiunta di orientamento sessuale, di dati genetici e di dati biometrici.

I dati non sensibili e non giudiziari prendono il nome di **dati comuni**.

Perché proteggerli?

Si vuole apprestare uno speciale **presidio** a informazioni con spiccato profilo di **rischio** per l'interessato.

Sono dati **intrinsecamente pericolosi**.

- Dati volti a consentire la libera collocazione della persona nella società.
- Identità sociale, politica, spirituale, sessuale.
- No a ingerenze indebite, no a costrizioni, no a pubblicizzazioni forzate, no a strumentalizzazioni.

Dati biometrici

- Le **fotografie** costituiscono dato biometrico solo quando sono trattate in modo tale da consentire l'identificazione univoca o l'autenticazione dell'interessato. Altrimenti sono dati personali **comuni**. (Bolognini, Giuffrè).

Elementi componenti della biometria: **i)** tipologia di utilizzo, **ii)** funzione, **iii)** fonte e **iv)** oggetto.

Identificazione e autenticazione

Tipologia di utilizzo: i dati biometrici sono impiegati di regola come **identificativi esclusivi**.

Funzione: assolvono funzione di identificazione e di autenticazione.

Fonte: sono estrapolati da caratteristiche fisiche, fisiologiche o comportamentali di una persona.

Oggetto: recano informazioni uniche sulla persona da cui sono estratte, ottenute con particolari tecniche di misurazione e di analisi matematica (Bolognini, Giuffrè).

Sistemi di sicurezza biometrici

Nella tradizione in tema di privacy e misure di sicurezza, i sistemi biometrici sono sempre stati collegati a un processo di **autenticazione.**

Qualcosa che tu conosci, qualcosa che tu possiedi, qualcosa che tu sei.

Reale sicurezza dei sistemi biometrici e **hacking** dei sistemi consumer (CCC).

Matematica

Informazioni **matematiche** elaborate a partire dal volto della persona, dalle impronte digitali, dalle caratteristiche dell'iride, da conformazione di reticoli o capillari, da elementi misurabili del modo di camminare o di gesticolare (Bolognini, Giuffrè).

Nuovo rapporto uomo/macchina

Cambiano in maniera irreversibile la relazione tra **corpo** e **identità**, in quanto le caratteristiche del corpo umano possono essere lette da una macchina e sottoposte a un successivo trattamento.

Decisioni del Garante sull'uso di sistemi biometrici: **extrema ratio**, dignità, capacità di controllo del lavoratore

Dati relativi alla salute

Dati sanitari

Sia salute **fisica**, sia mentale.

- Stato passato, presente e futuro, quindi anche valutazioni **prognostiche**.
- Anche identificativi personali utilizzati a fini sanitari, quali un codice o un simbolo, sono considerati dati sanitari (Bolognini, Giuffrè).

Tipi di dati sanitari (Bolognini, Giuffrè)

- Informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica
- Dati genetici e campioni biologici
- Informazioni su malattia, disabilità, rischio di malattie, anamnesi medica, trattamenti clinici, stato fisiologico o biomedico dell'interessato,
- Indipendentemente dalla **fonte** (medico o altro operatore sanitario, ospedale, dispositivo medico, test diagnostico in vitro).

Dati genetici

Sono una specificazione dei dati sanitari

- **Fonte**: sono estratti da campioni biologici della persona.
- **Oggetto**: recano caratteristiche genetiche, ereditarie o acquisite.

Dati sensibili per inferenza

I dati sensibili possono essere desunti da informazioni di per se stesse **non sensibili**

È stato considerato **dato personale sensibile** la scelta di un passeggero di prenotare un particolare **menù** da consumare in volo diverso dal menù standard, posto che da siffatta scelta possono inferirsi appartenenze religiose o filosofiche o intolleranze alimentari (Bolognini, Giuffrè).

Dati giudiziari

Dati relativi a condanne penali e reati

3. Non siamo in un paese per dati

Il concetto di ambiente ostile per i dati

Riguarda le **difficoltà** nel raggiungere una sicurezza reale dei dati e delle informazioni in un determinato ambiente

Il caso “El Chapo”

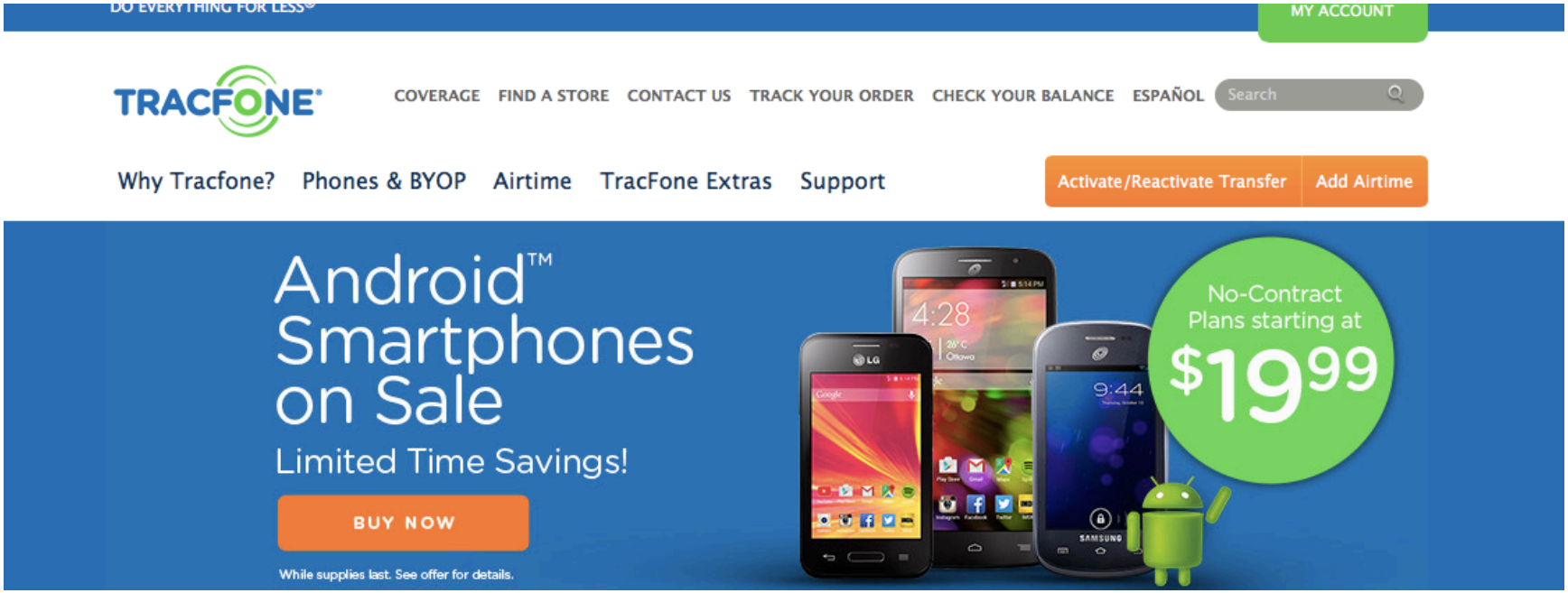
“Operations Security” (OPSEC)

- Sean Penn lascia **tutti i suoi dispositivi** a Los Angeles (quindi: sono **insicuri per definizione**).
- Utilizzo di TracFones e di BlackPhones (Silent Circle) (quindi: utilizzo di **strumenti ad hoc**).

OPSEC #2

- Uso di indirizzi e-mail anonimi e messaggi lasciati in bozza e non spediti, in account condivisi in chiaro (quindi: **comportamenti ad hoc**).
- Comunicazione con BBM (BlackBerry Messages) a intermediari (quindi: attività di **anti-forensics**).

TracFones


DO EVERYTHING FOR LESS®
MY ACCOUNT
TRACFONE
COVERAGE
FIND A STORE
CONTACT US
TRACK YOUR ORDER
CHECK YOUR BALANCE
ESPAÑOL
Search
Why Tracfone?
Phones & BYOP
Airtime
TracFone Extras
Support
Activate/Reactivate Transfer
Add Airtime
Android™ Smartphones on Sale
Limited Time Savings!
BUY NOW
While supplies last. See offer for details.
No-Contract Plans starting at
$19.99

Caratteristiche

- Economici (20 dollari) e affidabili (Motorola/ Samsung/LG).
- Prepagati.
- Nessun contratto, nessun collegamento utente/ SIM, nessuna richiesta di carta di credito.
- Ricaricabili.
- Numero intercambiabile o sempre lo stesso.
- Diffusione internazionale (oltre 100 località).

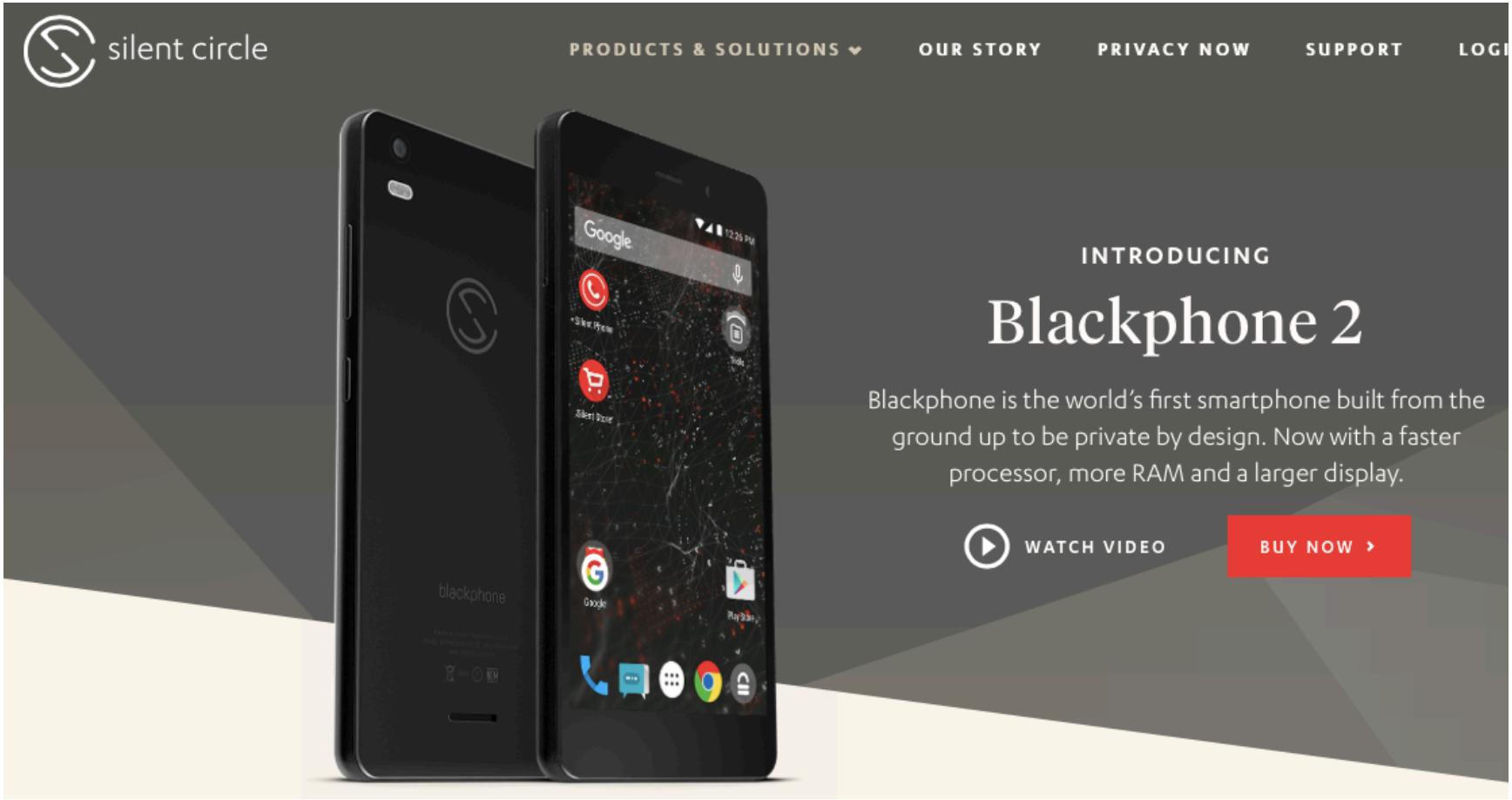
TracFones VIP

Katie Holmes Used a Disposable Cell Phone to Escape From Tom Cruise

Louis Peitzman
7/10/12 9:35pm · Filed to: TOMKAT

129.0K 81 2

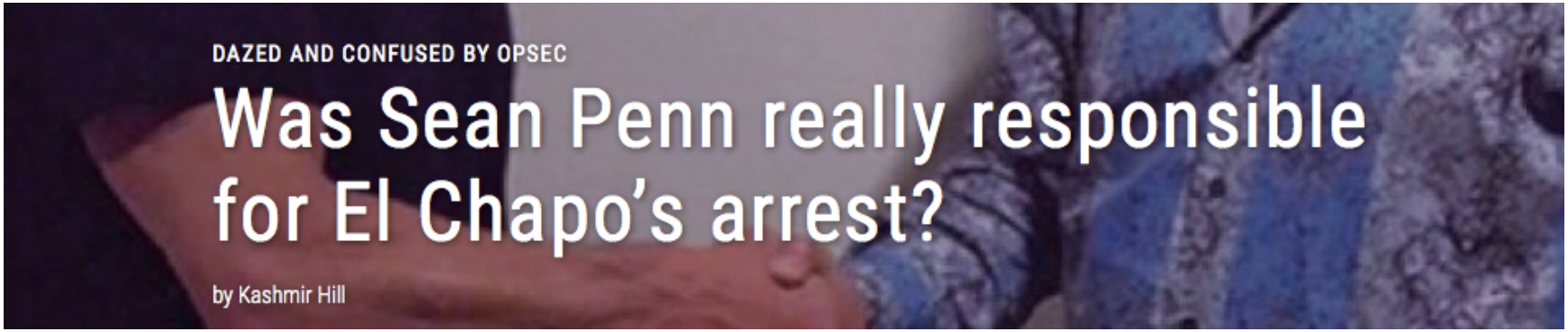
BlackPhones



Le caratteristiche

- Informazioni **cifrate** e messaggi **sicuri**.
- Si collega solo a reti wireless **certificate**.
- Un team risolve le **vulnerabilità** scoperte nel sistema operativo in 72 ore.
- Crea diversi telefoni **virtuali** che non condividono tra loro spazi comunicanti.

Ha influito nel tracciamento?



Mirroring dei dati con BBM

- Vuoi contattare il Boss? Manda BBM (messaggio da BlackBerry) a un **intermediario**, che se ne sta in un luogo pubblico connesso a un Wi-Fi.
- L'intermediario **trascrive** il testo su un iPad e lo manda attraverso il network (e non la rete cellulare).
- Chi lo riceve lo **trascrive** in un altro BBM e lo manda a **Guzman**. Quasi impossibile analizzare il traffico di Guzman perché comunica con solo un altro dispositivo e gli intermediari si spostano e cambiano continuamente.

Prime conclusioni:

- Nel digitale tutto si complica e spesso occorrono **strumenti ad hoc** per proteggere i dati.

- Raggiungere riservatezza reale, inviare lettere (e-mail) anonime, mantenere canali di comunicazione sicuri è di solito più complesso rispetto a quanto siamo abituati a fare nel mondo reale.

(b)

I dati e i comportamenti

Importanza di questo aspetto

- Oggi è l'aspetto più **importante** della sicurezza informatica.

- Anche la tecnologia più sofisticata è vulnerabile, e le banche dati più sicure diventano accessibili, se i **comportamenti** sono sbagliati.

Perché si sbaglia?

- Ignoranza degli aspetti più “profondi” delle tecnologie che utilizziamo e delle modalità di custodia e di protezione dei dati.

- Mancata **consapevolezza** degli effetti della circolazione del dato digitale.

Il concetto di “ambienti ostili”

- Ambienti non conosciuti.
- Ambienti che tracciano spostamenti o memorizzano i dati.

Policy

- Le policy sono di solito gli strumenti pensati per disciplinare i comportamenti.

- Molto **diffuse** anche negli studi professionali e molto “apprezzate” dal GDPR.

Morte della privacy

- Difficoltà di garantire la protezione del dato in un contesto dove sono le persone stesse a **diffondere** i loro dati o a violare la privacy altrui.

- Rinuncia a proteggersi e **esibizione** del dato.

Seconde conclusioni:

- **NON** siamo in un periodo storico votato alla privacy e alla riservatezza dei dati.
- Non sempre possiamo **controllare** tutti i nostri dati anche se NOI adottiamo comportamenti sicuri.
- È praticamente impossibile vivere “fuori dal sistema”.

(c)

Come operare in concreto

Una **policy** per la gestione quotidiana dei dati

1. La “comprensione” del dato

Capire il dato che si sta trattando e il suo “peso”.

Avere chiaro il suo **impatto** sulla privacy (nel nuovo Regolamento è previsto espressamente). Valutare il tipo di dato e analisi del rischio

Evitare **l’esposizione** dei dati volontaria e involontaria

Differenza tra dati **in chiaro** e **dati cifrati**.

Dati in chiaro e dati cifrati

La **crittografia** come strumento essenziale.

Nel file system, nei telefoni, nelle comunicazioni, nelle immagini e video.

Pericolo: il caso di TrueCrypt.

2. La cancellazione del dato

- Cancellazione **sicura** e recupero dei dati.
- Smaltimento dei rifiuti tecnologici, per il legislatore sulla privacy.
- Erasing o wiping dei dati.

3. Il backup

- Backup e **ridondanza** dei dati.
- Anche per la protezione dal **ransomware.**
- Sistemi di backup moderni e in tempo reale

4. L’antivirus e il firewall

Oggi essenziali come strumenti di protezione dei dati.

Attacchi nuovi e sempre più diffusi.

5. L’autenticazione

Unica sicurezza, a volte, per l’accesso ai dati.

Tutta la sicurezza sulla **password**.

Evoluzione dei **tre tipi** (conoscere, avere, essere).

6. I dati e i comportamenti

I comportamenti e il lato umano.

I tipici comportamenti sbagliati, e la **paranoia** come virtù.

7. Non violare la privacy altrui

Attenzione ai dati **di terzi**.

Prevedere anche l'uso anche **sbagliato** delle tecnologie che faranno coloro che si **relazionano** con noi.

8. La persistenza del dato

Persistenza e visibilità del dato.

Non vi è la possibilità di tornare **indietro**.

Diritto all'oblio tecnico **inesistente**.

9. Il finto anonimato

Il vero anonimato è assai difficile da raggiungere. Lo è anche per i dati. Per le informazioni delle persone.

Strumenti utili: **Tor** (per usi leciti).

Accesso alla rete e **mantenere** l'anonimato i due aspetti più difficili.

10. Conosci l’ambiente dei dati

- La conoscenza tecnica su come i dati sono trattati e l’hacking come strumenti di **vantaggio**.

- Di solito è complesso da far comprendere ai **giuristi** (si pensi al tema delicato delle vulnerabilità).

- Conoscenza dei database, delle tecniche di cifratura, della differenza tra IP statici e dinamici, delle procedure di data mining e di profilazione.

4. GDPR: rendere i dati anonimi

Anonimizzazione dei dati

Considerando 26

“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”.

L’anonimato non è semplice

- Informazione anonima: è l’informazione che non riguarda una persona fisica identificata o identificabile
- Anonimizzazione: è un trattamento cui sono sottoposti i dati personali volto a ottenere la de-identificazione irreversibile del soggetto a cui l’informazione si riferisce
- Deve avere caratteristiche di **irreversibilità**.

Dato anonimo: no GDPR

- L'informazione anonima si pone **al di fuori** della disciplina regolamentare.
- Non si applicano le relative disposizioni.
- Si colloca al lato **opposto** del dato personale
- La linea di demarcazione tra anonimo e identificabile è mobile, varia col tempo e con le tecnologie.
- Può esserci un anonimato solo **apparente**. (Bolognini, Giuffrè)

Deve essere **realmente** anonimo

Non basta che sia privo di **nome**.

- Sono informazioni che possono circolare liberamente e quindi possono essere un **patrimonio** di conoscenza, ma anche **economico**, molto importante.
- L'eliminazione di identificativi evidenti, come il nome o l'immagine, da un gruppo di dati personali risulta raramente sufficiente ad assicurare l'anonimato (Bolognini, Giuffrè).

Le migliori tecniche

- L’incrocio di informazioni può far cadere una anonimizzazione **mal impostata**
- Particolari tecniche di analisi o di Osint
- WP art. 29 ha **analizzato**: tecniche di randomizzazione, di generalizzazione, strumenti quali l’aggiunta di rumore statistico, le permutazioni, la privacy differenziale, l’aggregazione, il (k)anonimato, la (l)diversità, la (t)vicinanza.

Dato pseudonimizzato

Interruzione **momentanea** e **selettiva** del collegamento

«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;

Riduzione dei rischi

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.

Minor grado di rischio

- Sarebbe un tipo di trattamento **meno rischioso** per l'individuo, più sicuro e protetto da violazioni
- Un minor grado di rischio che dà così al contempo maggiori margini di azione a chi raccogli dati

Privacy enhancing

Tecnica di **privacy enhancing**: il trattamento avviene in modo che le informazioni che consentono ai dati di essere attribuiti a una persona identificata siano conservate **separatamente** rispetto al dato pseudonimizzato generato e siano soggette a misure tecniche e organizzative che assicurino tale **non attribuzione**

Chiavi di re-identificazione

I dati non sono immediatamente riconducibili all'interessato (**interruzione** momentanea).

Occorrono delle chiavi di **re-identificazione**.

5. Il dato in PRATICA

CODAU

Linee guida in materia di privacy e protezione dei dati personali in ambito universitario (**Versione 1.1 – novembre 2017**)

Università degli Studi di Milano Statale, Università degli Studi di Milano Bicocca, Università degli Studi di Firenze, Politecnico di Milano, Università degli Studi di Messina, Università di Bologna.

Privacy by design del dato e del sistema

Attiene le **buone prassi** di protezione dei dati personali sin dalla **progettazione** del trattamento.

Misure strumentali

i) la migliore applicazione del principio di **minimizzazione** dei dati personali oggetto del trattamento con riferimento tanto alla quantità dei dati, tanto ai **tempi** di conservazione e ai livelli di accessibilità, tanto alle prefissate finalità;

Misure strumentali #2

ii) la pseudonimizzazione ovvero l'oscuramento (**reversibile**) dei dati identificativi del soggetto interessato;

Misure strumentali #3

iii) definizione di dati personali e **tempi** strettamente necessari al trattamento, in relazione alle diverse finalità.

Il “proprietario” dei dati

L’interessato (data subject) è la persona fisica alla quale si riferiscono i dati trattati.

È sempre una **persona fisica**.

L’interessato è quindi il soggetto “**proprietario**” dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento.

Il GDPR al Capo III elenca nel dettaglio tali diritti.

I diritti

Alcuni di questi, a seconda della finalità per la quale i dati sono stati raccolti, potrebbero **non** essere esercitabili dagli interessati.

Per esempio non è possibile effettuare la cancellazione dei dati relativi alla carriera di uno studente perché devono essere conservati illimitatamente per pubblico interesse, mentre può essere accolta la richiesta di cancellazione dei **recapiti personali**.

Risposte alle richieste sui dati

La risposta alle richieste dell'interessato deve comunque essere **tempestiva** e, anche nel caso non sia possibile soddisfarla, occorre specificare la **motivazione** del rifiuto.

Il titolare ha il compito di facilitare l'accesso all'interessato ai suoi dati, predisponendo dei canali di comunicazione dedicati, quali ad esempio i recapiti del **Responsabile della Protezione dei Dati**.

Descrizione dei trattamenti

Per la descrizione dei trattamenti si usa raggruppare gli **interessati** in **categorie omogenee** a seconda del tipo di rapporto che questi hanno con il titolare.

In ambito universitario si possono individuare le seguenti principali categorie d'interessati, le quali possono poi essere suddivise in **sottocategorie** per distinguerle all'interno di alcuni trattamenti:

Categorie

- Studenti.
- Personale tecnico-amministrativo.
- Personale docente.
- Collaboratori.
- Assegnisti.
- Dottoranti.
- Specializzandi.
- Fornitori.
- Clienti.
- Privati cittadini.

Mappa dei dati e dei trattamenti

Si è ritenuto opportuno stilare una **mappatura** dei principali trattamenti che trovano svolgimento in ambito universitario con l'obiettivo di:

Registro dei trattamenti

1) Consentire di completare in modo più agevole il **registro dei trattamenti**, tenuto conto del fatto che gran parte dei dati personali e delle finalità del trattamento sono **comuni** a molti Atenei;

Rapporti con interessato

2) Individuare le informazioni che dovranno essere comunicate **all'interessato**, con particolare riferimento agli aspetti introdotti nel nuovo GDPR (es: indicazioni sui tempi di conservazione dei dati, finalità indicate in modo specifico), condividendo ove possibile alcune bozze di informative;

Peculiarità

3) Mettere in evidenza alcune **peculiarità** del trattamento dei dati preso in esame ed eventuali considerazioni fatte in merito ai principali dubbi interpretativi.

Elementi considerati

1. La natura dei dati

L’analisi sulla **natura dei dati** consente di determinare se, e in quale misura, possono essere trattati (come ad esempio: categorie **particolari** di dati personali di cui all’’art. 9 e/o i dati relativi a condanne penali e reati di cui all’art. 10), evidenziando eventuali **accorgimenti** adottati da alcuni Atenei nel trattamento di tali dati.

2. Dati strettamente necessari

L’analisi sui tipi di dati che sono **strettamente necessari** per perseguire un obbligo legale o di quelli strettamente **connessi** all’esecuzione di **compiti istituzionali** favorisce la definizione di tempi di conservazione differenti o la previsione di differenti garanzie per l’interessato.

3. Modalità per informativa e consenso

Tenuto conto del nuovo GDPR, nonché dell'obbligo di indicare nell'informativa "la base giuridica del trattamento" e "i legittimi interessi perseguiti dal titolare del trattamento" si ritiene opportuno fornire all'interessato **maggiori dettagli** sulle finalità.

3. #2 Modalità consenso

Sono quindi condivise anche alcune valutazioni in merito all'opportunità di raccogliere un consenso *ad hoc* per le **diverse finalità** non connesse a obblighi legali o allo svolgimento di compiti strettamente istituzionali.

4. Archiviazione e conservazione

(Tempi, modi, quali dati)

L'informativa sulla privacy dovrà indicare il **periodo** di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

Tale informazione è utile anche nell'ambito della redazione dei **registri di trattamento**: sarà infatti importante determinare i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

I trattamenti possono essere compiuti con o senza l'ausilio di processi automatizzati.

5. Note sui diritti dell'interessato

Si è ritenuto opportuno esplicitare in questa sezione alcune note inerenti i **diritti** dell'interessato.

6. Categorie di interessati

Categorie di interessati

Le categorie di **persone fisiche** cui si riferiscono i dati personali. Ad esempio: studenti, personale dipendente, collaboratori, fornitori, ospiti.

7. Categorie di destinatari

Categorie di destinatari

È previsto individuare nell'informativa le categorie di destinatari a cui i dati personali possono essere comunicati.

Categorie destinatari #2

Si dovrà quindi dare indicazione di tutte le persone che possono ricevere comunicazione di dati personali (es: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che possono venire a conoscenza dei dati, nonché, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali).

Nelle schede di trattamento sotto riportate, non sono stati indicati eventuali soggetti esterni che potrebbero trattare i dati in qualità, ad esempio, di amministratori di sistema o di rete o di database, considerato che tale informazione è strettamente connessa all'organizzazione dei singoli Atenei.

In relazione ai destinatari, si specifica inoltre che, 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, occorre chiarire - nell'informativa privacy - le possibili **conseguenze** della mancata comunicazione dei dati.

8. Comunicazione e trasferimento all’estero

Occorre chiarire nell’informativa l'intenzione del titolare del trattamento di **trasferire dati personali** a un paese terzo o a un'organizzazione internazionale.

Tale dato è rilevante anche nell’ambito della redazione del registro, pertanto, si è ritenuto opportuno effettuare alcune note e approfondimenti su tale aspetto.

Un esempio

Trattamento finalizzato per l'erogazione del percorso formativo e gestione della carriera (dall'immatricolazione alla laurea)

Descrizione del trattamento

Il dato è trattato per permettere la gestione degli eventi inerenti la carriera dello studente, quali la gestione del piano di studio, la registrazione degli esami e la domanda di laurea.

Natura dei dati

Personali, categorie particolari di dati personali (stato di salute), dati personali relativi a condanne penali e reati.

Dati personali strettamente necessari

Dati anagrafici, di contatto, dati per la verifica dei requisiti e inerenti la carriera (es: titoli, valutazione di prove intermedie, prova finale).

In funzione della provenienza dello studente potrebbero rendersi necessari ulteriori dati (esempio: informazioni sul permesso di soggiorno).

Vengono gestite anche altre informazioni non obbligatorie in termini generali ma richieste in situazioni specifiche: dati bancari, ISEE, fotografia, contatti telefonici, contatti email personale/i).

Finalità

Sono di seguito descritte le principali finalità di trattamento di dati sensibili e/o dati personali relativi a condanne penali e reati:

a. Dati relativi agli studenti e/o a familiari diversamente abili o ad elementi reddituali ai fini di un eventuale controllo sulle **autocertificazioni** relative alle tasse universitarie e di eventuali esoneri dal versamento delle tasse universitarie e/o fruizione di eventuali agevolazioni previste dalla legge, nonché dati relativi alla gestione dei contributi straordinari per iniziative degli studenti;

b. dati relativi allo status di rifugiato per la fruizione di esoneri e borse di studio;

c. dati relativi allo stato di gravidanza al fine di attuare tutte le cautele necessarie per la tutela della donna in stato di gravidanza, sia per motivi didattici, quali la frequenza di laboratori, sia al fine della fruizione di eventuali agevolazioni e benefici di legge;

d. Dati idonei a rivelare le opinioni politiche o l’adesione a partiti, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale per esigenze connesse allo svolgimento delle procedure elettorali interne all’Ateneo;

e. Dati sensibili e dati personali relativi a condanne penali e reati che si rilevano nell'ambito di procedimenti disciplinari a carico degli studenti;

f. dati relativi alla propria condizione di salute per attività di mediazione del rapporto con i docenti, attività di interpretariato, tutorato, trasporto e servizi analoghi per tutti gli studenti con disabilità o disturbi specifici dell'apprendimento.

Modalità per l’informativa e il consenso

È redatta un’unica informativa e non è necessario acquisire il consenso.

Archiviazione e conservazione

(tempi, modi, quali dati)

- L'anagrafica degli studenti e i dati di carriera sono conservati dall'Ateneo illimitatamente nel tempo
- I dati inerenti graduatorie o verbali sono conservati illimitatamente nel tempo
- La conservazione dei restanti dati è sotteso ai tempi di conservazione degli atti amministrativi che li contengono.

Note sui diritti dell'interessato

In merito alla cancellazione dei dati – non può essere concessa la cancellazione di dati personali che, per la normativa vigente o in ragione di regole d'Ateneo previste nei massimari o nei regolamenti interni:

- possono essere cancellati solo successivamente alla data di richiesta dell'interessato
- devono essere conservati illimitatamente nel tempo.

In merito alla rettifica dei dati, deve essere concessa la **rettifica del sesso**, soprattutto a fronte di una sentenza che stabilisca l'avvenuto cambio di genere.

Categorie di interessati

- Studenti.
- Familiari (solo a fini dell’esercizio al diritto allo studio).

Categorie di destinatari

- Strutture interne dell'Ateneo preposte quali, ad esempio, Segreterie Studenti, Uffici di Segreteria Didattica, Scuole, Dipartimenti, strutture preposte alla Comunicazione.
- Responsabili di trattamento: eventuali fornitori di servizi per uso di canali social (es. gruppo ex-alumni); società che stampano le pergamene di laurea; ecc..
- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

Enti locali ai fini di eventuali sussidi a favore di particolari categorie di studenti

Avvocatura dello Stato, Ministero degli Affari esteri, Questure, Ambasciate, Procura della Repubblica relativamente a permessi di soggiorno, al riconoscimento di particolari status

- Enti di assicurazione per pratiche infortuni
- Organismi Regionali di Gestione (Enti dotati di autonomia amministrativo-gestionale istituiti ai sensi delle norme vigenti in materia di diritto agli studi universitari) ed altri istituti per favorire la mobilità internazionale degli studenti, ai fini della valutazione dei benefici economici e dell'assegnazione degli alloggi
- Agenzia Entrate per 730 nel caso di dottorandi o specializzandi

- MIUR
- Soggetti pubblici e privati per consentire agli studenti di fruire di agevolazioni, sussidi e servizi. Al fine di favorirne l'integrazione nel territorio e nell'ambiente universitario, possono altresì essere comunicati i dati inerenti agli studenti di scambio a enti, istituti o associazioni

- Finanziatori di premi, borse di dottorato e assegni, anche stranieri, nel caso di studenti e/o dottorandi che abbiano usufruito di finanziamenti.
- Atenei stranieri, impegnati in percorsi formativi con rilascio di titoli congiunti.
- Servizi penitenziari.

Comunicazione e trasferimento all'estero

I dati inerenti agli studenti di scambio possono essere traferiti, su richiesta a:

- Autorità all'estero (nel caso in cui sia necessario verificare il titolo di studi per ragioni professionali o per prosecuzione degli studi)
- Ambasciate all'estero (anche per esoneri dal servizio militare)
- Università extra UE (nell'ambito di scambi internazionali per studenti in-going e out-going)

6. La morte del dato (e il futuro…)

La morte ti fa social…

L’annuncio è stato dato il 13 marzo 2016 dalla **BBC**

«A breve, su Facebook, ci saranno più **morti** che **vivi**. Il social network per eccellenza ha già preso le sembianze di un **cimitero digitale**, in costante e inarrestabile crescita».

Chi muore si rivede…

Oltre **trenta milioni** i profili online che apparterrebbero già a persone scomparse.

8.000 decessi digitali al giorno.

Quasi **un milione** di morti digitali “residenti” negli Stati Uniti d’America.

Nel **2065** – o, al massimo, nel 2095 – si registrerà il **sorpasso**: più account di morti che vivi.

In Italia

240.000 morti digitali in un anno, con un trend di **650** bacheche abbandonate a loro stesse ogni **giorno**, su un parco utenti che ammonterebbe a circa 24 milioni.

Gli aspetti da toccare

Temi sociali, tecnologici, storici, religiosi e filosofici, sino ad arrivare a delineare all'orizzonte una **nuova idea** di comprensione e gestione della morte **ripensata** ed **adattata** per l'era digitale e per le numerose identità virtuali, o **corpi elettronici**, dell'individuo.

Anche la security

È un settore in grado di sollevare problemi **pratici**, quesiti tecnologici, di hacking e di sicurezza informatica e **controversie legali** che sono già di grandissima attualità.

Che ruolo avrà la security del futuro sulla **morte** del dato o, meglio, sul **controllo** del processo di morte del dato (e del relativo tracking)? Si pensi al **Regolamento Europeo** e al suo tentativo di tenere sotto controllo gli spostamenti delle informazioni.

Cosa ne sarà dei dati?

Il primo elemento di analisi riguarda la **comprensione** – che sia la più lucida possibile – di che cosa ne sarà dei dati digitali **dopo la morte**.

Il corpo elettronico?

Quale sarà il destino di tutte le persone/identità digitali/**alter ego virtuali**/corpi elettronici che hanno preso forma nel corso di **anni** di attività online?

Quali saranno le **persone** che potranno disporne e che, in ultima istanza, potranno prendere delle **decisioni** sul modo in cui trattare i beni digitali?

Visibili per sempre?

I multiformi contenuti dei profili sui social network, dei blog e delle caselle di posta elettronica resteranno per sempre **visibili a tutti** e, quindi, supereranno anche la morta fisica dell'utente, rimanendo **eterni**?

Fissi o in movimento?

E rimarranno eterni **fissi**, o eterni in **movimento**?

In altre parole: saranno **congelati** e **cristallizzati** al momento esatto del decesso dell'utente o potranno essere **aggiornati** costantemente da parenti o amici e rimanere, in un certo senso, **vivi**?

E se li voglio eliminare?

Al contrario, se uno **non** volesse rimanere eterno, avrà la possibilità di **eliminare** tutti i dati e le sue tracce digitali per sempre?

Di far sì, in altre parole, che le informazioni **muoiano** insieme a lui?

Automazione

Magari, di poterlo fare in maniera **automatizzata** – ad esempio come conseguenza diretta della morte fisica – nel caso, per ipotesi, si registrasse un periodo più o meno lungo di **inattività**, cancellando i dati definitivamente o mantenendoli in rete ma impedendo **l'accesso** da parte di chiunque?

Si pensi a un pulsante "rimuovi tutti i dati" in servizi quali **SugarSync** o **CrashPlan** o simili.

Ci dobbiamo rassegnare?

Dobbiamo **accettare** il fatto e **rassegnarci** all'idea che siamo ormai in un'epoca di dati **eterni**, che sopravvivono senza difficoltà anche alla morte dell'individuo o, al contrario, abbiamo ancora dei margini di **possibilità** per, ad esempio, predisporre processi di **autodistruzione** dei dati quale **ultima forma** di tutela della privacy e dei nostri segreti?

Non è solo questione di profili

Ridurre la questione della morte digitale – e della relativa eredità – a un problema di gestione di **profili**, account, ricordi, video o immagini e alla cura di qualche status o galleria di selfie è a dir poco **riduttivo**.

Corpo elettronico

Oggi i dati in rete – e spesso sono online da decenni, e si sono pian piano **accumulati** nel corso del tempo – sono in grado di creare un **alter ego** che ha sempre di più assunto la forma di un **corpo elettronico** e che cresce e si sviluppa di pari passo con le attività online della persona.

Patrimonio

Infine, non meno importante, può assumere rilievo l'aspetto strettamente **patrimoniale**. La presenza costante in rete genera, oggi, **economia** e acquisti di beni e di servizi.

Quali sono i **metodi migliori** per gestire un patrimonio informativo che ogni giorno **aumenta** e che, nella vita di una persona, arriva ad assumere quasi sempre un valore economico (o **emozionale**) ingente?

Stima

Si pensi, ad esempio, a una stima, seppur approssimativa, dei beni e servizi che un utente medio **acquista** in rete ogni anno. Questo è l'aspetto più vicino all'idea diffusa che si ha di **eredità**, sia da un punto di vista tradizionale, sia in un'ottica strettamente giuridica: un patrimonio di beni, accumulato nel tempo, che assume un valore non solo affettivo ma anche **economico**.

I soggetti interessati

Sono oggi **tre** le categorie particolarmente interessate all'evoluzione del tema della morte digitale:

- i politici/ legislatori,
- i gestori delle piattaforme di social network
- i notai.

Piattaforme

I fornitori di piattaforme di social network e i provider di servizi di posta elettronica e di spazi sul cloud cercano, quotidianamente, di **mediare** tra le esigenze di **privacy** dei clienti/utenti defunti e le istanze di parenti e amici per **ottenere** i dati di un parente deceduto o per **celebrare**, anche online, il ricordo di una persona.

Come operano:

Le aziende mirano ad **anticipare** la volontà dell'utente, dando la possibilità ai clienti di nominare, con "**finti testamenti**", degli **eredi** digitali, cristallizzando un profilo facendolo diventare **commemorativo** e **immodificabile** (una lapide, o tempietto digitale) o, ancora, **conservando** i tweet o i messaggi scambiati in una sorta di **memoria digitale postuma** e accessibile a chi dimostrerà di averne diritto.

Esigenze degli eredi

Come si può riuscire ad accedere ai dati del parente defunto, ad esempio, se l'azienda che li gestisce – si pensi a un grande **provider** di account di posta elettronica, anche gratuito – decide di **non** collaborare e, per di più, ha la sede **all'estero**?

Morte (anche) digitale

Allo stesso tempo, però, ci può essere chi **non vuole** rimanere visibile ma desidera, invece, **cancellare** tutti i suoi dati e disattivare account e profilo. Può esistere chi, in altre parole, oltre che morire da un punto di vista **fisico**, desideri morire anche da un punto di vista **digitale**.

Oblio

Infine, è evidente, un terzo aspetto connesso a doppio filo a mortalità e immortalità digitale è la ricerca di un **oblio elettronico**, nella maggior parte dei casi assai **difficile** da ottenere.

Come può agire, infatti, chi **non** vuole essere immortale? Chi vuole **cancellare** le informazioni che lo riguardano anche finché è in vita, e non solo dopo la morte?

Terreno di scontro

La lotta per l'oblio è diventata estremamente **complessa** ma coinvolge, anch'essa, aspetti molto importanti della natura umana nel mondo digitale.

L'oblio in sé è un istituto che è molto **delicato** da trattare. È sicuramente un diritto, ma può entrare in **conflitto** con la libertà di informazione e di cronaca e, in senso lato, con il diritto di **conoscere** fatti e informazioni.

Si tratterà, a mio avviso, del terreno di **scontro** più **importante** dei prossimi anni tra diritto e tecnologia.

Facebook

La funzione denominata **Memorial**.

Permette di trasformare le pagine di un utente in un **account commemorativo**, ossia in uno spazio dove solo le conoscenze più strette possono intervenire con post o commenti.

In pratica, la pagina dell'utente defunto viene "**cristallizzata**" e ne è limitata la possibile interazione verso l'esterno.

Death proof

Per attivare un profilo commemorativo occorre inviare a Facebook una **death proof**, una prova scritta della morte dell'utente – ad esempio un certificato di morte, o la fotografia di un necrologio, o la dichiarazione di un notaio – e il profilo è **congelato** e reso commemorativo o, a scelta dei parenti, **rimosso**.

Due opzioni

Sono, quindi, **due** le opzioni che Facebook concede esplicitamente ai parenti o agli amici cari di un utente morto che abbia attivo un profilo sul social network:

i) renderlo **commemorativo**, o

ii) domandarne la **rimozione** dal social network affinché non sia più visibile a nessuno.

No credenziali

Non è invece possibile – a meno che uno non sia, ovviamente, in possesso delle credenziali dell'utente, ma il **sostituirsi** a un'altra persona e operare con le sue password è ritenuto scorretto da tutte le regole contrattuali delle piattaforme – domandare a Facebook di **poter entrare** nel profilo privato dell'utente per conoscere ciò che era, appunto, privato (quali e-mail e messaggi), a meno che non vi sia l'ordine specifico di un magistrato.

In anticipo

Su Facebook è indicato chiaramente come l'utente possa indicare in **anticipo** se desidera che l'account sia reso un domani commemorativo o, invece, sia eliminato completamente dal social network.

Google

Google, per gestire il problema della **morte** online, ha per ora previsto **due** strategie complementari: la gestione dei cosiddetti "**account inattivi**" – account che "non danno segni di vita" per un certo periodo – e la più tipica possibilità, per i parenti, di domandare la **cancellazione** di un account di una persona deceduta testimoniandone, con specifici documenti, il decesso.

Esecutori testamentari

Al contempo, ed è l'aspetto più importante, Google consente di scegliere fino a dieci "**esecutori testamentari**" o, meglio, "esecutori dell'account", che dovranno prendere delle scelte su quell'account in caso di morte del titolare e che, ovviamente, potranno seguire le **istruzioni** ricevute dallo stesso.

Potere dei delegati

Google permette all'utente di fornire maggiori **poteri** ai "delegati", che potranno avere **accesso**, se l'utente vorrà, a tutte le informazioni, comprese e-mail, fotografie e documenti sul cloud.

Twitter

Anche Twitter ha delineato da tempo una procedura molto chiara su come gestire gli account di utenti deceduti. Il sistema adottato è noto per la sua **semplicità**.

«In caso di decesso di un utente Twitter, possiamo collaborare con una persona autorizzata ad agire per suo conto o con un familiare stretto e verificato del defunto per **disattivare** l'account».

No credenziali!

Subito dopo la descrizione della procedura da seguire, è pubblicata in grande evidenza una nota:

«Nota: non siamo in grado di fornire le credenziali di accesso dell'account a nessuno, indipendentemente dal suo rapporto con il defunto».

Portarsi i dati nella tomba

Molti utenti sono in rete da tanti anni e hanno accumulato una grande quantità di dati; si è venuta, così, a costituire una vera e propria "**vita digitale**", connessa a un'identità digitale – o a una seconda/terza personalità che dir si voglia – che si è **arricchita** giorno dopo giorno e che ha visto un'evoluzione sensibile e inarrestabile negli ultimi anni.

Cifratura

Per dati quali video, fotografie o documenti riservati, la cosa migliore è, ovviamente, collocarli su un disco, o su un altro tipo di supporto ben **individuabile** e in possesso dell'utente, e **cifrarli** applicando un software di **crittografia** o attivando le funzioni di cifratura che ormai tutti i sistemi operativi prevedono.

Wiping

Un secondo metodo, più radicale, per far sì che nessuno possa entrare in possesso dei dati è la **distruzione completa** e **sicura** delle informazioni utilizzando determinati tipi di software che non permettano più in alcun modo il recupero delle informazioni cancellate.

Dove sono i dati?

In questo caso, occorre essere sempre a conoscenza di **dove siano** i dati che si vogliono distruggere, accertarsi che non ve ne siano altre **copie** in circolazione e poi procedere con cura alla loro distruzione.

Difficili da individuare

Purtroppo ci sono molti dati che riguardano la persona che non sono così **facilmente** individuabili, e che diventano molto difficili da nascondere a curiosi per il semplice motivo che non si ha né la **disponibilità**, né il **controllo** su di essi.

Backup

Si pensi alle e-mail **custodite** da un provider sui suoi server, o ai dati posizionati su un servizio di cloud.

Per di più, si tratta di servizi che, per motivi di sicurezza, di solito effettuano anche costanti **backup** (copie di sicurezza) in chiaro, quindi il dato tende a moltiplicarsi e a essere **ridondante**.

E questo, da un punto di vista della sicurezza, può **non** essere un bene.

Piano di distruzione

È possibile, in definitiva, prevedere **un piano di distruzione** soltanto di quei dati che siano ben **localizzati** e che, soprattutto, siano nel **possesso** della persona.

La cancellazione dei dati sui dispositivi personali, sul telefono, sul tablet è comunque già un **ottimo** punto di partenza.

Non si può garantire, invece, la **completa distruzione** di dati che stanno circolando in rete a nostra insaputa, o al di là delle nostre possibilità di **tracciamento** e di **controllo**.

Pena di morte digitale

Un aspetto tecnico molto interessante che riguarda la morte del dato e, in alcuni casi, dell'intera persona online – o corpo elettronico che dir si voglia – è **la chiusura improvvisa** di un profilo, di un servizio o di un account a seguito di un **atto unilaterale** del provider.

Spazi chiusi improvvisamente

Si pensi a un social network che decide di chiudere un profilo che ha agito in violazione delle regole contrattuali, o al fornitore di uno spazio sul cloud contenente migliaia di dati altrui che non **rinnova l'abbonamento** perché non è stato corrisposto il canone annuale e distrugge le informazioni o, ancora, a un'utenza che non è rinnovata dal titolare stesso, magari per **dimenticanza**, e perde tutti i dati.

Pena di morte

Nel caso non si siano effettuati dei **backup** e il provider non abbia previsto la **riconsegna** dei dati al termine del servizio, vi è il rischio concreto che quei dati siano stati eliminati **per sempre** insieme alla persona digitale correlata.

Spegnere interruttore

La realtà è che molti dei contratti dei più moderni servizi che si approvano – spesso senza leggere con attenzione le clausole – prevedono la **possibilità**, per l'azienda, di interrompere **improvvisamente** il rapporto e di cessare **immediatamente** la fornitura del servizio.

Clausola cloud

Si veda, per fare un esempio, la seguente **clausola** di un servizio di cloud.

«**Risoluzione**. Ci riserviamo il diritto di sospendere o terminare i Servizi in qualsiasi momento a nostra discrezione e senza previo avviso. Ad esempio, potremmo sospendere o terminare l'utilizzo dei Servizi se non rispetti i presenti Termini, se utilizzi i Servizi in modalità che potrebbero causarci conseguenze legali o interrompi i Servizi o l'utilizzo degli stessi da parte di altri utenti».

PEC

Una seconda ipotesi realistica ancora più spiacevole che potrebbe accadere si potrebbe collegare a un **servizio critico**.

Un account di posta elettronica certificata (PEC).

Contratto

Il contratto che il professionista accetta quando attiva una casella di posta elettronica prevede, nella maggior parte dei casi, sia l'ipotesi di **sospensione** del servizio, sia la più preoccupante opzione della **cessazione** del servizio.

In molti contratti si trova una facoltà di risoluzione del contratto senza preavviso, ovviamente in capo al provider, che opera prima **sospendendo** l'account per dare al professionista la possibilità di accedere alla casella per scaricare i messaggi e, poi, **comminando** un divieto di accesso definitivo.

Estate

Facciamo l'ipotesi, allora, che il titolare della casella di posta elettronica certificata commetta un'infrazione attorno alla metà del mese di agosto e che venga avvertito dalla società, tramite PEC, che ha **48** ore di tempo per scaricare tutte le sue e-mail certificate.

Vacanza

Nel caso il professionista fosse in vacanza o, comunque, in un luogo impossibilitato ad accedere all'account, al ritorno in ufficio scoprirebbe di avere **perduto** tutte le e-mail certificate e qualsiasi comunicazione o notificazione contenuta nella sua vecchia casella di posta.

Entro 48 ore

Il riferimento alle 48 ore di tempo per recuperare tutta la e-mail è, però, reale ed è previsto da alcuni servizi.

Una previsione che, in caso di qualche contrattempo, potrebbe generare un'ipotesi di **morte digitale** di dati così importanti.

Percezione della fragilità

Manca, in molti utenti, la percezione che gran parte dei servizi che si utilizzano quotidianamente, soprattutto quelli gratuiti, potrebbero essere **sospesi** o **cancellati** da un momento all'altro con gravi conseguenze se i dati che si sono accumulati nel corso dell'anno sino a quel momento non erano stati memorizzati da altra parte.

Il dato al centro

Capacità di **diffusione**, di **trasformazione**, di **correlazione** e di **resistenza** alla cancellazione che sono molto particolari e che devono essere correttamente interpretate.

La security si **può** e si **deve** fare carico anche di questo aspetto.

GRAZIE!!

Giovanni Ziccardi

giovanni.ziccardi@unimi.it

http://www.ziccardi.org