e-privacy XX 2016

Gli ecosistemi delle professioni legali tra privacy e big data nelle normative italiana e europea

Avv. Nicola Fabiano
(Studio Legale Fabiano)

STUDIO LEGALE
FABIANO

Big Data

Big data *è il termine usato per descrivere una raccolta di dati così estesa in termini di* ***volume****,* ***velocità*** *e* ***varietà*** *da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore.*

Big data rappresenta anche l'interrelazione di dati provenienti potenzialmente da ***fonti eterogenee****, quindi non soltanto i dati strutturati, come i database, ma anche non strutturati, come* ***immagini****,* ***email****,* ***dati GPS****, informazioni prese dai* ***social network****.*

Fonte: Wikipedia

Internet: i dati

3,456,143,882

Internet Users in the world

1,079,818,968

Total number of Websites

85,017,322,139

Emails sent today

1,822,153,034

Google searches today

1,695,237

Blog posts written today

237,932,731

Tweets sent today

4,246,998,881

Videos viewed today
on YouTube

24,024,483

Photos uploaded today
on Instagram

37,516,015

Tumblr posts today

THE INTERNET IN REAL TIME

Days Hours Minutes Seconds

0 0 : 0 0 : 0 0 : 1 5

Jump to... 1 Hour 1 Day 1 Month

share the love

Facebook
Active users: 10,049
Log onto: 198,702
New profiles: 95
Video views: 1,458,340
Photos uploaded: 54,684

Instagram
765,623
Likes

Twitter
114,219
New tweets

Snapchat
27,342
People using service

Youtube
1,975,145
Video views

Pinterest
2,552
Articles pinned

Tumblr
Signups: 16
Posts: 9,718
Blogs: 32
Visitors: 1,213
Revenue: $ 47

Cloud storages
$22,225
Capitalisation

The Internet in Real Time

By the time you finish reading this sentence, there will have been 219,000 new Facebook posts, 22,800 new tweets, 7,000 apps downloaded, and about $9,000 worth of items sold on Amazon… depending on your reading speed, of course. Now that the Internet is widely available, just one second of global online activity is jam-packed full of events, from communication with others to data storage to entertainment options galore.

For example, in the amount of time you've been on this page, this is how much data has already passed through the Internet.

307,200

GIGABYTES OF DATA

The amount of data uploaded to the Internet in a single second is a staggering 24,000 gigabytes. Cisco forecasts that monthly Internet data will reach 91.3 exabytes – or 1 billion gigabytes – by the year 2016, pushing the amount of online activity even higher.

Want to know what else happens in single second online? Scroll down to find out what has happened on the Internet just since you loaded this page!

I multipli del byte secondo le unità del Sistema Internazionale (SI) delle unità di misura

Nome	Simbolo	Multiplo
Kilobyte	KB	10^3
Megabyte	MB	10^6
Gigabyte	GB	10^9
Terabyte	TB	10^{12}
Petabyte	PB	10^{15}
Exabyte	EB	10^{18}
Zettabyte	ZB	10^{21}
Yottabyte	YB	10^{24}

40 Zettabytes
(43 trilioni di GB) nel 2020
- Fonte IBM -

Volume
Quantità di dati

Variety
Differenti tipologie di dati

Dati sulla salute
Dati dei Social Network
Video - Facebook -
Twitter

Le 4 V dei Big Data

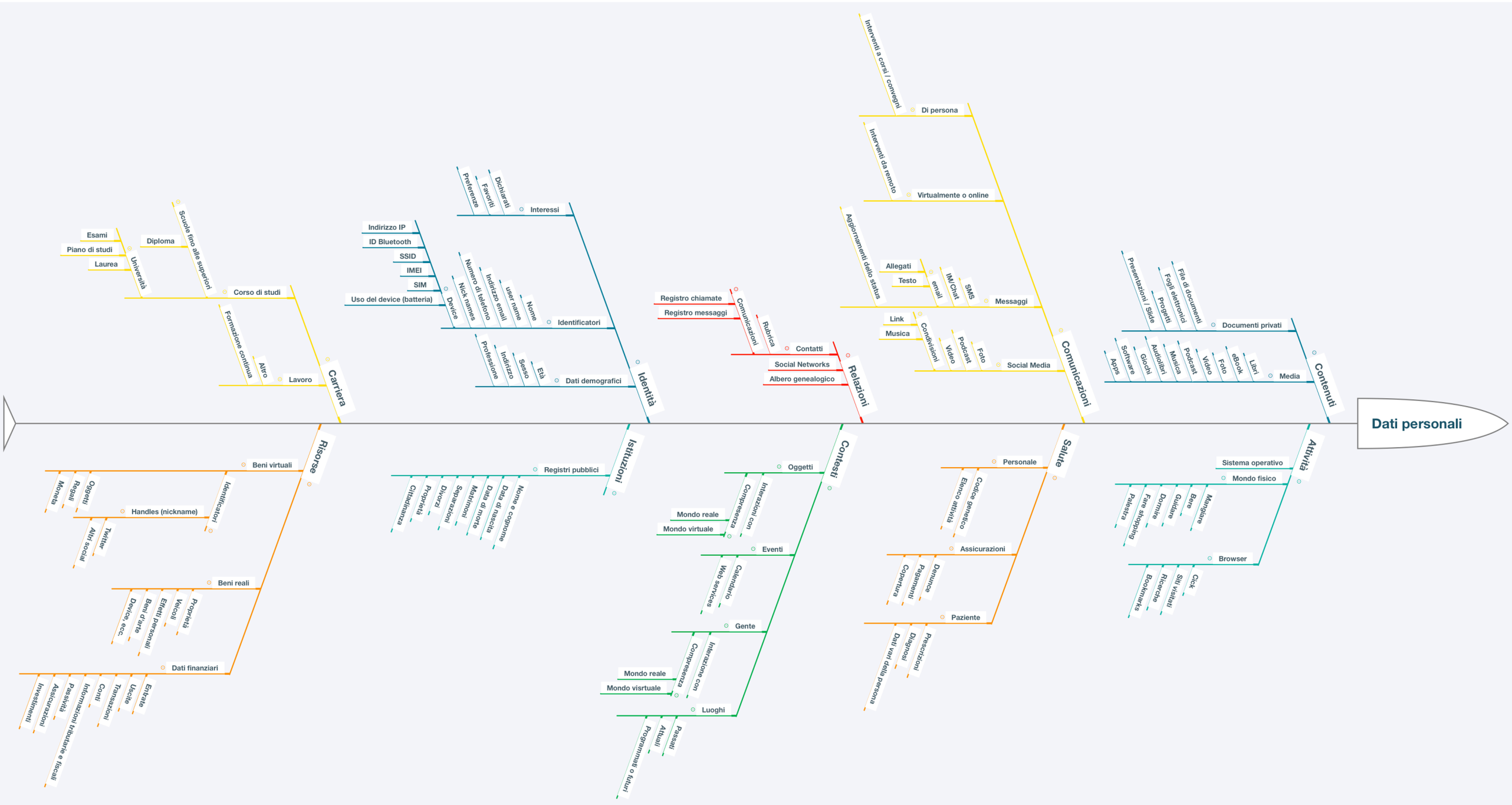
Velocity
Rapida elaborazione

Veracity
Qualità dei dati

Nel 2016
18,9 bilioni di reti connesse
- Fonte IBM -

Percentuale molto bassa
di corrispondenza per
interoperabilità e
affidabilità

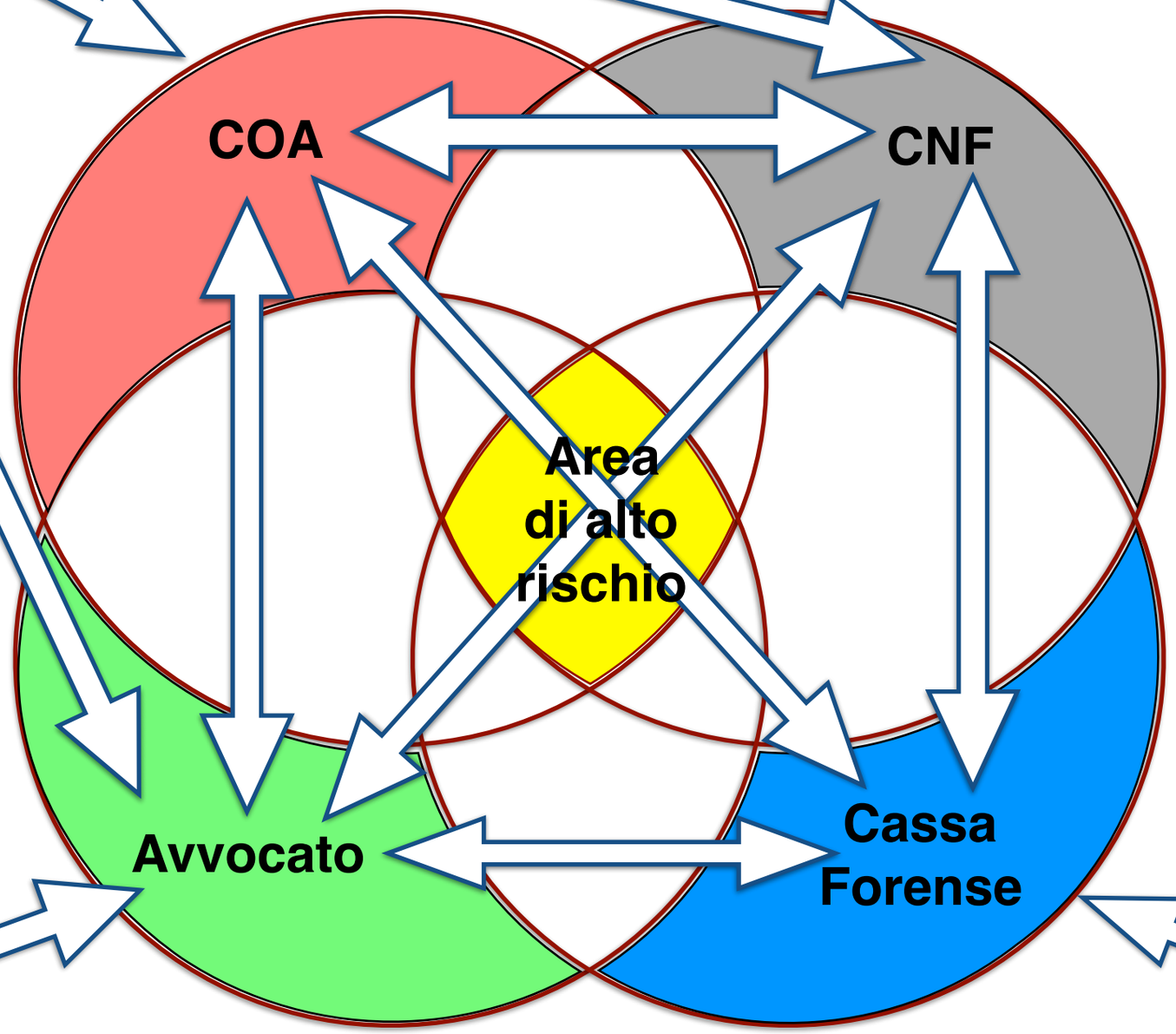
Mappa esemplificativa delle aree relative ai dati personali



Gli ecosistemi delle professioni legali

L'analisi

PA
e altri soggetti



Proiezione della graduazione del rischio

Si tratta di un insieme di relazioni complesse tra sistemi con reciproche interazioni; ne derivano trattamenti di dati personali e gestione delle informazioni.
Rilevano la modalità di trasmissione dei flussi di dati e le caratteristiche del modello relazionale ove applicabile.

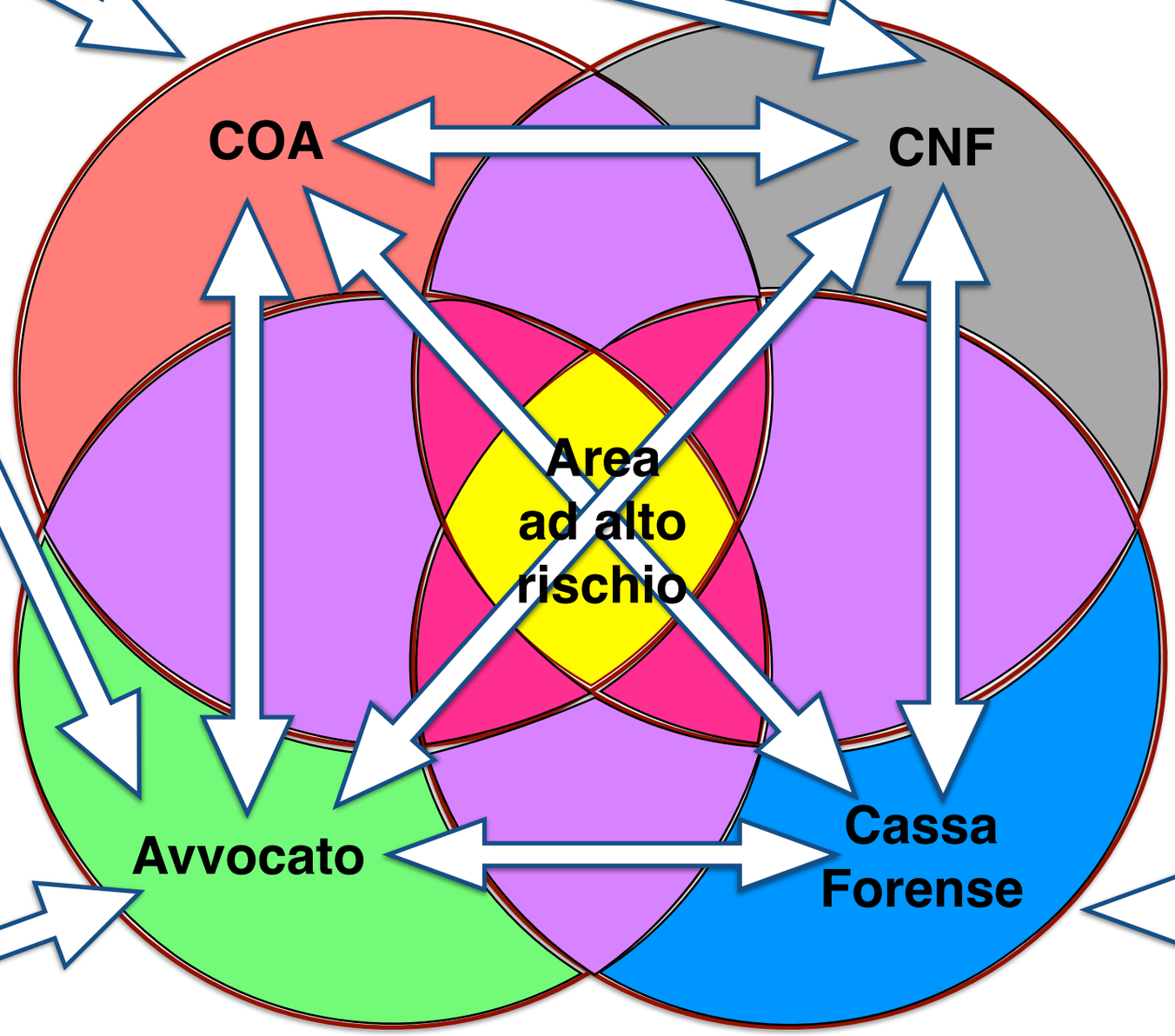
Clienti

PA
e altri soggetti

Dove risiedono i dati e come vengono veicolati ?

Gli ecosistemi delle professioni legali

PA
e altri soggetti



Graduazione del rischio in funzione dei soggetti che trattano i dati e di altri parametri come la quantità di informazioni, ecc.

Clienti

PA
e altri soggetti

Dove risiedono i dati e come vengono veicolati ?

Principali questioni

1. dove risiedono i dati e come vengono trattati;
2. quali misure di sicurezza;
3. la comunicazione dei dati;
4. analisi dei dati e dei flussi;
5. analisi di graduazione del rischio e quindi;
6. valutazione DPIA;
7. approccio DPbDbD (PbD);
8. evitare violazioni dei dati (*data breach notification*).

Analisi comparata
di alcune norme nazionali ed europee
sulla protezione dei dati personali

Il "DATO"

D.Lgs 196/2003	Regolamento UE 679/2016
Art. 4 - Definizioni	**Articolo 4 - Definizioni**
*"**dato personale**": **qualunque informazione** relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.*	«**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.*

Il consenso

D.Lgs 196/2003

Art. 23. Consenso

1. Il **trattamento** di dati personali da parte di privati o di enti pubblici economici **è ammesso solo con il consenso espresso dell'interessato**.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Regolamento UE 679/2016

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;

…

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.

…

Il trattamento

D.Lgs 196/2003

Art. 11 - Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:

a) **trattati in modo lecito e secondo correttezza**;

b) **raccolti e registrati** per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;

c) **esatti** e, se necessario, aggiornati;

d) **pertinenti, completi e non eccedenti rispetto alle finalità** per le quali sono raccolti o successivamente trattati;

e) **conservati in una forma che consenta** l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Regolamento UE 679/2016

Art. 5 - Principi applicabili al trattamento di dati personali

1. I dati personali sono:

a) **trattati in modo lecito**, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) **raccolti per finalità determinate, esplicite e legittime**, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) **esatti e, se necessario, aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) **conservati in una forma che consenta** l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) **trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

…

Infografica dal sito del Garante privacy

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Data protection by design and by default

D.Lgs 196/2003

N U L L A

Regolamento UE 679/2016

Articolo 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, **sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso** il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la **pseudonimizzazione**, volte ad attuare in modo efficace i principi di protezione dei dati, quali la **minimizzazione**, e a **integrare nel trattamento le necessarie garanzie** al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. **Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.** In particolare, dette misure garantiscono che, **per impostazione predefinita**, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Profili di responsabilità e sanzioni

Il risarcimento dei danni

D.Lgs 196/2003

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Regolamento UE 679/2016

Articolo 82 - Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

D.Lgs 196/2003 - sanzioni amministrative

Violazione	Sanzione
Omessa o inidonea informativa	*da € 6.000,00 a € 36.000,00*
Cessione dei dati dopo la cessazione del trattamento	*da € 10.000,00 a € 60.000,00*
Comunicazione di dati che rivelano lo stato di salute	*da € 1.000,00 a € 6.000,00*
Violazione delle misure minime di sicurezza o per il trattamento illecito	*da € 10.000,00 a € 120.000,00*
Inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto	*da € 30.000,00 a € 180.000,00*
Violazione del diritto di opposizione	*da € 10.000,00 a € 120.000,00*
Omessa o incompleta notificazione	*da € 20.000,00 a € 120.000,00*
Omessa informazione o esibizione al Garante	*da € 10.000,00 a € 60.000,00*

D.Lgs 196/2003 - sanzioni penali

Violazione	Sanzione
Trattamento illecito	*reclusione da 6 a 18 mesi*
Comunicazione o diffusione dei dati	*reclusione da 6 a 24 mesi*
Trattamento illecito di dati che presenta rischi per i diritti e le libertà fondamentali	*reclusione da 1 a 3 anni*
Falsità nelle dichiarazioni e notificazioni	*reclusione da 6 mesi a 3 anni*
Omessa adozione delle misure minime	*arresto sino a 2 anni*
Inosservanza dei provvedimenti del Garante	*reclusione da 3 mesi a 2 anni*

Le sanzioni del Regolamento UE 679/2016

Articolo 83 - Condizioni generali per infliggere sanzioni amministrative pecuniarie

…

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie **fino a 10.000.000 EUR**, o per le imprese, **fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

a) **gli obblighi** del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
b) **gli obblighi** dell'organismo di certificazione a norma degli articoli 42 e 43;
c) **gli obblighi** dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore:

a) **i principi di base del trattamento**, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
b) **i diritti degli interessati** a norma degli articoli da 12 a 22;
c) **i trasferimenti di dati personali** a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
d) **qualsiasi obbligo** ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
e) **l'inosservanza di un ordine**, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, **l'inosservanza di un ordine da parte dell'autorità di controllo** di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000 EUR**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore.

…

Al di là dell'obbligo normativo,

il dato personale

ha un valore economico

ma deve essere valutato e considerato

come un valore assoluto.

Grazie per l'attenzione

Avv. Nicola Fabiano

n.fabiano@studiolegalefabiano.eu

http://www.studiolegalefabiano.eu

nicfab **nfabiano** **nicfab**

STUDIO LEGALE
FABIANO