MOVIMENTO FORENSE
PER UN'AVVOCATURA
INDIPENDENTE
AUTONOMA
LIBERA

Verso il Regolamento Europeo sulla protezione dei dati personali

GDPR: storia e principi

Perugia, 11 maggio 2018

Palazzo Cesaroni, Sala Brugnoli

Avv. Filippo Bianchini

Apocalittici o integrati?

- Il 98% delle informazioni raccolte dagli umani nel mondo è registrato in formato digitale.

  (Martin Hilbert, Associate Professor at University of California)

- In media le persone danno un'occhiata allo schermo dello smartphone per 150 volte al giorno.

  ("*Internet Trends Report*" by Klaunier Perkins Caufield & Byer's)

- Il telefono è parte dell'anatomia umana.

  (The Supreme Court of the United States, Riley vs. California: *"[…] now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy*")

- Kosinski (Cambridge Analytica) sostiene che siano sufficienti informazioni su:

  - 70 “Mi piace” messi su Facebook, per sapere più cose sulla personalità di un soggetto rispetto ai suoi amici;

  - 150, per saperne di più dei genitori del soggetto;

  - 300, per superare le conoscenze del suo partner.

  Con una quantità ancora maggiore di “Mi piace” è possibile conoscere più cose sulla personalità rispetto a quante ne conosca il soggetto stesso.

Dato personale

- “Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); […] direttamente o indirettamente” (art. 4)

  Ad esempio:

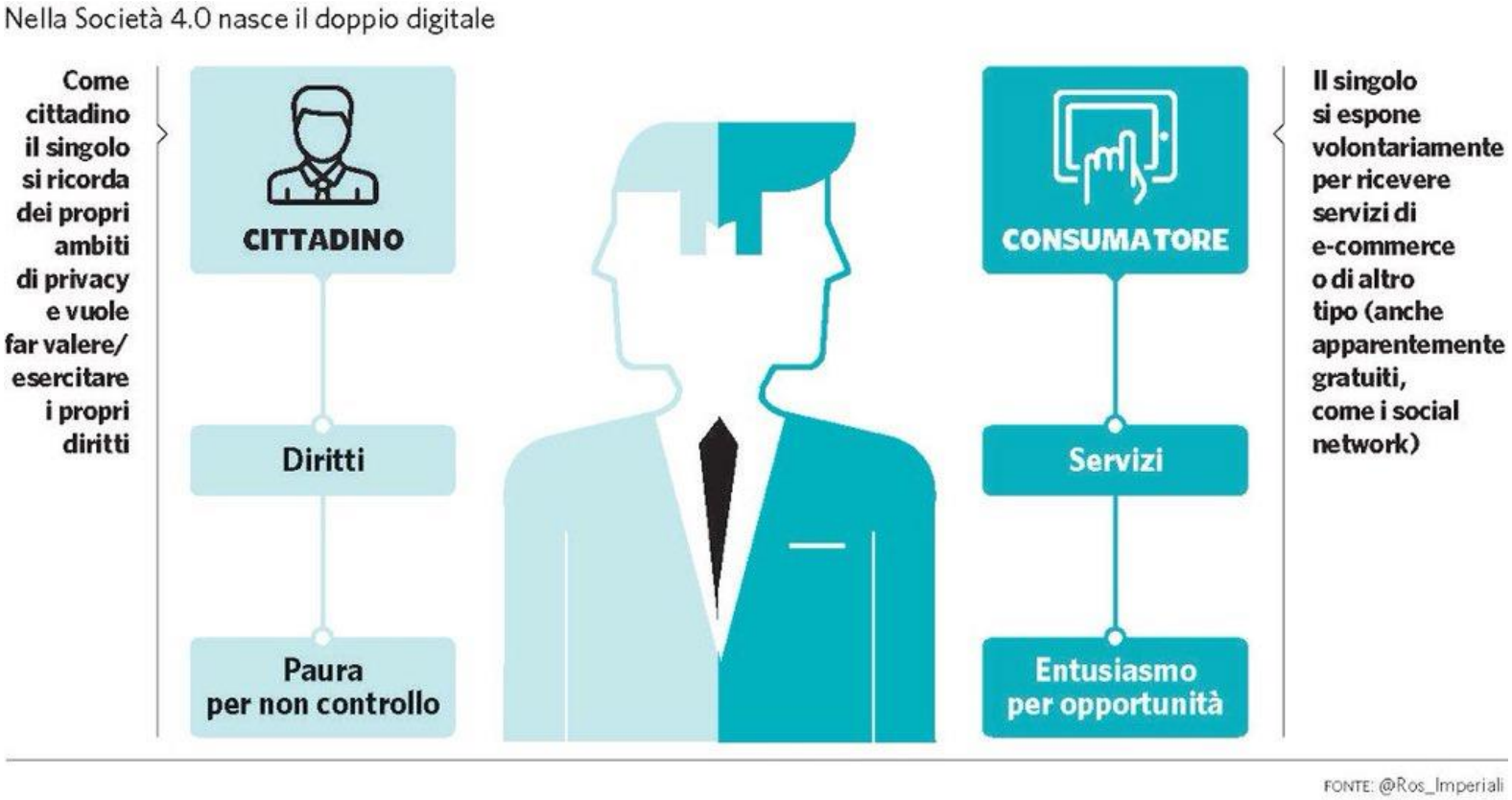
  - nome
  - numero identificazione (C.F., matricola)
  - dati relativi all’ubicazione (GPS, tag RFID)
  - identificativo online (login, IP, cookies)
  - elementi caratteristici dell’identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (immagine, impronta, iride, comportamento, etnia, convinzioni filosofiche e religiose)

COM'È OGGI IL DATO?

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**: rende il tracking dell'informazione complesso (si pensi al cloud e allo **spostamento costante di informazioni** anche in base alle esigenze/risorse del sistema).

(Bolognini-Pelino-Bistolfi, *Il Regolamento Privacy europeo*, Giuffrè)

Il doppio digitale



Il rischio-dati

- La digitalizzazione ha portato con sé un dono del quale si farebbe volentieri a meno: il rischio concreto che i nostri dati possano essere trafugati in qualunque istante.

  - In casa (smart tv, domotica, elettronica a bordo dell'auto)

  - A scuola (registri elettronici, test scolastici)

  - In ospedale (aggiornamento firmware – il S.O. – di 745mila pacemaker a rischio hacker prodotti da San Jude Medical)

  - In ufficio (PEBCAK: *Problem Exists Between Chair And Keyboard*)

Dati… a bordo


Internet
Web-based Services
Cellular 3G/4G
Bluetooth BLE NFC
Radio
HD Radio
Phone Projection
XM GPS
Wi Fi
V2I - DSRC
Electric Vehicle Charging Station
Service Shop
Counterfeit Parts
V2V - DSRC
Wireless Sensors (e.g., TPMS, RKE)
Internal Propagation of Attacks Introduced via USB, SD, Disc, etc.

Il petrolio del nuovo millennio

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules

The Economist

May 6th 2017

Il valore dei dati

- **Economico**:
  - dati finanziari (carte di credito, credenziali home banking, ecc.);
  - dati personali (identità, sanitari, lavorativi, ecc.).
- **Strategico**:
  - dati che controllano il corretto funzionamento di sistemi critici e non;
  - dati che codificano informazioni riservate di tipo politico, militare, economico, industriale, ecc.

Quanto valgono i **MIEI** dati?

- Calcolatore del valore dei dati personali: https://ig.ft.com/how-much-is-your-personal-data-worth/

  Il valore medio dei dati personali spesso ammonta a **meno di un dollaro** (*sic!*)

Proteggere i dati (ISO 27001)

- **Riservatezza** (*confidentiality*): i dati non sono disponibili o comunicati a parti non autorizzate
  - *Data breach*: compromissione della confidenzialità dei dati
- **Integrità** (*integrity*): i dati si trovano in uno stato di consistenza per tutto il loro ciclo di vita
  - *Data tampering* (*sabotage*): compromissione dell'integrità dei dati
- **Disponibilità** (*availability*): i dati sono disponibili in qualunque situazione (anche a fronte di eventi disastrosi)
  - *Data access denial*: compromissione della disponibilità dei dati

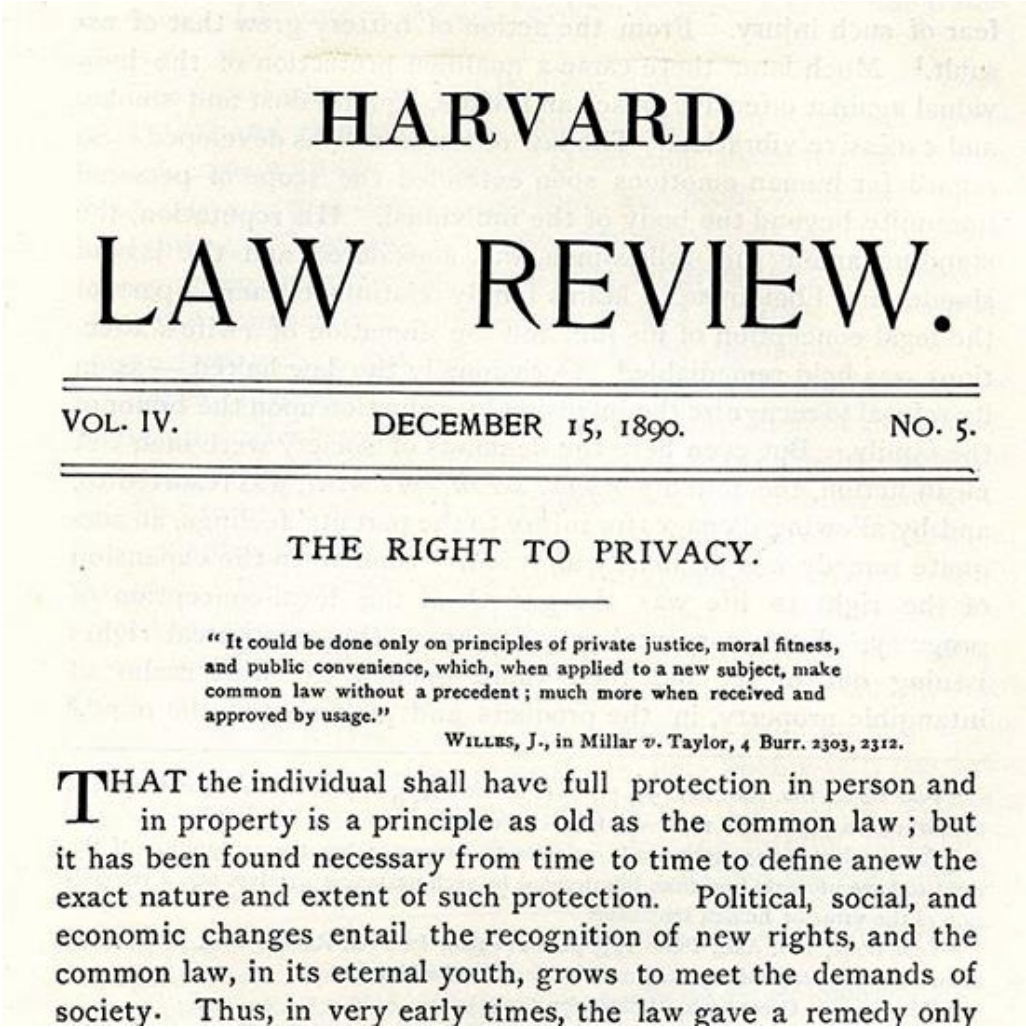
Parliamo di «Data protection», non di «Privacy»

- In nessuna parte del regolamento viene utilizzato il termine *privacy*.
- Se consultiamo il Cambridge Dictionary scopriamo che per *privacy* si intende "*someone's right to keep their personal matters and relationships secret*" o anche "*the state of being alone*".
- Si tratta di un diritto alla riservatezza che dipende dalla personale volontà del singolo di non rivelare informazioni relative alla sua vita privata.

- **Come ha inciso l'evoluzione tecnologica sul concetto di privacy?**

  Negli USA, nella seconda metà dell'800, ci si pose il problema di come tutelare la riservatezza degli individui a fronte di una straordinaria e rapida diffusione di informazioni tramite le stampa e le fotografie.

The Right to Privacy



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

Dal gossip sulle nozze nasce la parola ***privacy***

- Samuel Warren, brillante avvocato di Boston, dopo aver sposato nel 1883 la bella Mabel Bayard, al suo ritorno dal viaggio di nozze trovò decine di articoli invadenti giornalisti e paparazzi.
- Assieme a Louis Brandeis (che diventerà giudice federale nel 1916), partendo dallo *jus solitudinis*, con un famoso saggio pubblicato dalla Harward Law Review il 15 dicembre del 1890 intitolato *The Right to Privacy* coniò il concetto ed il termine giuridico: "*the right to be let alone*".

  (Dini, *La nuova privacy*, Il Sole 24 Ore)

Diverse tradizioni giuridiche

- Tradizione giuridica europea di **data protection** (protezione dei dati dei cittadini rispetto a chi li tratta in maniera automatizzata, v. schedatura FIAT) e non di **privacy** (modello americano) inteso come "*right to be let alone*" – c.d. *Transatlantic divide*
- Timothy Garton Ash, "*Il dossier*", Mondadori

- Quello che nel mondo americano nasce come *Right to privacy*, destinato a segnare i confini tra la sfera di riservatezza delle persone e il diritto fondamentale alla libertà di manifestazione del pensiero e di stampa, nel continente europeo si afferma invece come "*Diritto alla protezione dei dati personali*", inteso come diritto di libertà, legato al diritto dell'individuo a non essere sottoposto a controlli e raccolta di informazioni sulla propria vita senza il suo consenso o senza che sussistano ragioni di prevenzione o repressione di reati esplicitamente previsti dalle leggi.

  (Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Giappichelli)

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).

  (Ziccardi)

La privacy come diritto

- **La privacy è un diritto dell'uomo?**

  Per l'Europa sì, tanto che il diritto alla riservatezza per sé e la propria famiglia venne inserito nella Convenzione europea per i diritto dell'uomo del 1950.

Le tre tappe della tutela dei dati personali

- **1)** La Direttiva comunitaria **95/46/CE** ha fissato i principi generali della normativa in materia di dati personali per consentire la libera circolazione dei dati personali nel territorio europeo.

- **2)** Le Direttive Comunitarie **2002/58/CE** e **2009/136/UE** relative al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche hanno introdotto alcune precisazioni specifiche rispetto alla Direttiva 95/46 che riguardano la raccolta di dati personali effettuata on line e in particolare all'uso dei cookies.

- **3)** Nel 2012 la Commissione Europea ha deciso di adottare un Regolamento europeo per abrogare la direttiva 95/46 in materia di protezione dei dati personali e, per quanto riguarda il nostro ordinamento, anche le relative disposizioni contenute nel Codice in materia di protezione dei dati personali. Non tutte le norme del Codice saranno però abrogate, rimanendo inalterate quelle di attuazione della Direttiva 2002/58 e quelle della Direttiva 2009/136.

Perché una nuova normativa privacy Europea

- La norma cardine a livello UE in materia di protezione dati personali è la Direttiva 95/46/CE, adottata nel 1995 con l'obiettivo di:

  proteggere i diritti fondamentali e garantire il libero flusso di dati personali tra i Paesi Membri UE
- Nel tempo sono poi arrivate le normative privacy:

  - specifiche per il settore delle telecomunicazioni, la principale: Direttiva 2002/58/CE

  - la normativa privacy apposita per le istituzioni UE: Regolamento 45/2001
- Il trattamento dei dati personali è inevitabilmente presente al 99% in tutti i settori della nostra vita sociale e professionale.
- La creazione delle condizioni che agevolano e promuovono il business UE dipendono anche dalla normativa in materia di protezione dati personali, che gioca un ruolo essenziale - ora e nel futuro - per la *Digital Agenda for Europe* e più in generale per la *Europe 2020 Strategy*.

- Nel corso di questi anni

  - il trend della globalizzazione ed esternalizzazione dei servizi

  - gli sviluppi tecnologici

  - la nascita ed il successo di nuovi servizi della *Information and Networked Society*

  hanno totalmente cambiato il quadro di riferimento per le prescrizioni presenti nella direttiva privacy 95/46/EC entrate in vigore 20 anni fa.

- La direttiva privacy 95/46/EC con le sue 28 diverse trasposizioni nel paesi Membri UE ha comportato un quadro normativo frammentario e disomogeneo, che ha creato squilibri, condizioni di sbilanciamento e diversità di regole per le organizzazioni (aziende, enti, ecc.) che fanno business nella UE, ricomprese tra queste anche le organizzazioni extra UE.

Il "pacchetto privacy"

- A partire dal 2012 la Commissione Europea ha proposto al Parlamento ed al Consiglio Europeo una profonda revisione ed aggiornamento della normativa privacy europea
- Il primo fondamentale obiettivo raggiunto – *approvato dal Parlamento Europeo il 14 aprile 2016 – il Pacchetto di norme costituito da:*

  - Il Regolamento Privacy Europeo per la protezione degli individui con riferimento al trattamento dei loro dati personali e relativo libero flusso nella UE

  (abroga e sostituisce la Direttiva Privacy 95/46/EC)

  - La Direttiva privacy specifica per regolare la protezione dei dati personali da parte delle autorità competenti a fini di prevenzione, ricerca, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (in luogo della precedente apposita "Framework Decision 2008/977/JHA")

Dalla Direttiva al Regolamento

- La Direttiva 95/46/CE costituisce il primo corpo normativo che a livello comunitario è stato adottato per garantire la protezione dei dati personali
- "Direttiva" e non "Regolamento" in quanto vi era marcata disomogeneità tra i diversi Paesi membri, molti dei quali non avevano ancora nessuna norma specifica nel proprio ordinamento destinata a garantire la protezione dei dati personali e quindi si decise di lasciare margini più ampi al legislatore nazionale.

Entrata in vigore del Regolamento

- Approvazione ufficiale del Parlamento il 14 Aprile 2016.
- Regolamento n. 2016/679 pubblicato in GUCE n. 119 del 4 maggio 2016.
- Entrata in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale UE.
- Effettiva applicazione a decorrere da due anni dalla sua entrata in vigore.

- Nonostante il Regolamento generale non sia da recepire con normative nazionali, ci sono diversi aspetti che dovranno essere disciplinati dalla normativa interna di armonizzazione.
- Verosimilmente, il Garante dovrà, per ognuno dei Provvedimenti e Linee Guide di carattere generale emessi fino ad oggi, valutarne la "coerenza complessiva" e la conformità rispetto al Regolamento, dovendo quindi decidere se modificarli ovvero dichiararli non applicabili.

Elementi essenziali

- Abroga la direttiva europea 95/46/CE
- Non abroga (direttamente) il D.Lgs. n. 196 del 2003
- Non abroga i provvedimenti del Garante
- Disapplicazione di norme nazionali in contrasto con il regolamento
- Applicazione di norme nazionali derogatorie (ove ammesso), integrative, speciali

Coordinamento normativo

- Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone integrare elementi del regolamento nel proprio diritto nazionale (Cons. 8)

- Per quanto riguarda il trattamento dei dati personali […] per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del regolamento (Cons. 10)

Il quadro normativo applicabile in Italia

Regolamento 2016/679	**IN VIGORE,** pienamente applicabile dal 25 maggio 2018
Direttiva 1995/46	**IN VIGORE,** decade il 24 maggio 2018
Codice D.Lgs. 196/2003	**VIGORE, NON DECADE**, dovrà essere coordinato con il reg. UE secondo i criteri indicati dalla Legge di Delegazione
Provvedimenti Autorità Garante	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Accordi Internazionali su Trasferimento dati	**VIGORE, NON DECADONO,** fino a quando non verranno modificati, sostituiti, abrogati
Decisioni Commissioni UE	**IN VIGORE, NON DECADONO,** fino a quando non verranno modificate, sostituite, abrogate

Oggetto e finalità (art. 1)

- Il presente regolamento stabilisce norme relative alla protezione delle **persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
- Al centro del Regolamento vi è la persona: l'**interessato.**
- Ma la persona, e i suoi diritti di libertà, si proteggono attraverso la protezione dei suoi **dati.**
- È un elemento che **cambia** grazie alla società dell'informazione e dei social network.

Ambito di applicazione materiale (art. 2)

- Il regolamento si applica al trattamento interamente o parzialmente **automatizzato** di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Esclusioni

- Il regolamento non si applica ai trattamenti di dati personali:

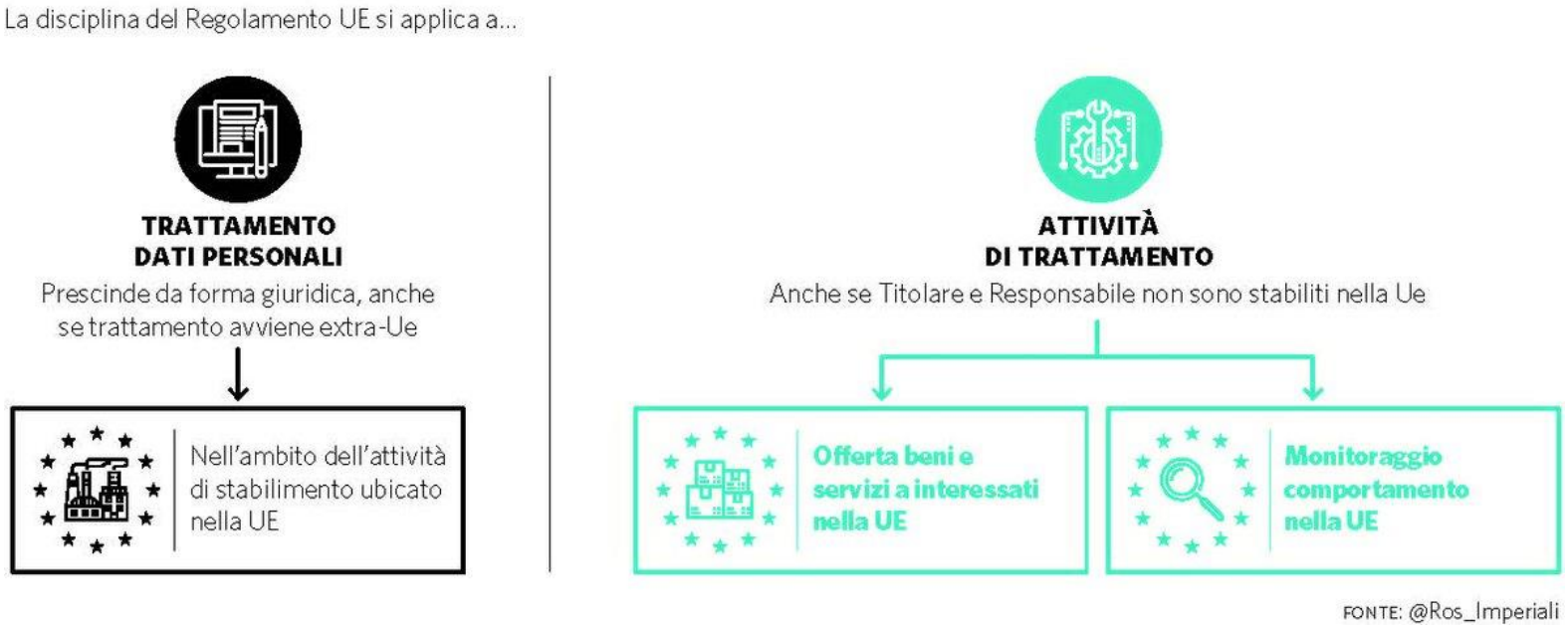
  a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

  b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

  c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

  d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Ambito di applicazione territoriale (art. 3): ultra-territorialità



Principi applicabili al trattamento di dati personali (art. 5)

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**»);

I dati personali sono:

- 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**»).

Accountability

- Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («**responsabilizzazione**»).

Direttiva vs Regolamento

	Direttiva 95/46	**Regolamento sulla protezione dei dati personali**
CONSENSO	possibile sia regime di opt-in che opt-out quindi anche forme "implicite"	È necessario che vi sia un forma "esplicita" ed inequivocabile
NOTIFICAZIONE	previsto l'obbligo di notificare alcune tipologie di trattamenti	Nessun obbligo; tutto demandato alla accountability ed alla PIA
TIPOLOGIE DEI DATI	personali sensibili giudiziari	I dati Sensibili diventano "Particolari"; Viene introdotta la definizione dei dati: **genetici;** **biometrici;** **pseudo-anonimi**;
DIRITTI DELL'INTERESSATO	conferma del trattamento, accesso ai dati, rettifica,cancellazione, limitazione e/opposizione per determinate finalità o operazioni di trattamento	**Diritto all'oblio;** **Diritto alla portabilità dei dati;**

Direttiva vs Regolamento

	Direttiva 95/46	Regolamento sulla protezione dei dati personali
TITOLARE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma molto light	Indicati gli oneri connessi alla titolarità: Privacy by design e by default; Misure idonee in relazione ai trattamenti; Autonoma valutazione dei rischi (PIA); Documentazione dei trattamenti e self assessment periodico di verifica.
RESPONSABILE DEL TRATTAMENTO	Definizione e ambiti di responsabilità descritti in forma INDIRETTA	Accountability diretta del Responsabile anche in ordine al risarcimento del danno; Contratto o altro atto giuridico per regolare i rapporti con il Titolare; Possibile impiego di sub-fornitori con delega del Titolare.
DATA PROTECTION OFFICER	Figura non prevista	Obbligatorio per la PA e in caso di monitoraggio regolare e sistematico su larga scala e trattamento su larga scala di dati sensibili e giudiziari; "suggerito" per gli altri Titolari in quanto figura che svolge un ruolo di cerniera nei confronti della Autorità; Esperto di protezione dati sia per gli aspetti legali che tecnici. Dipendente o Consulente con ampi margini di autonomia

Grazie per l'attenzione

Avv. FILIPPO BIANCHINI
Via Bontempi, 1
06122 PERUGIA

Tel.: (+39) 075 5723243
Fax: (+39) 075 5728372

E-mail: avv.filippobianchini@gmail.com