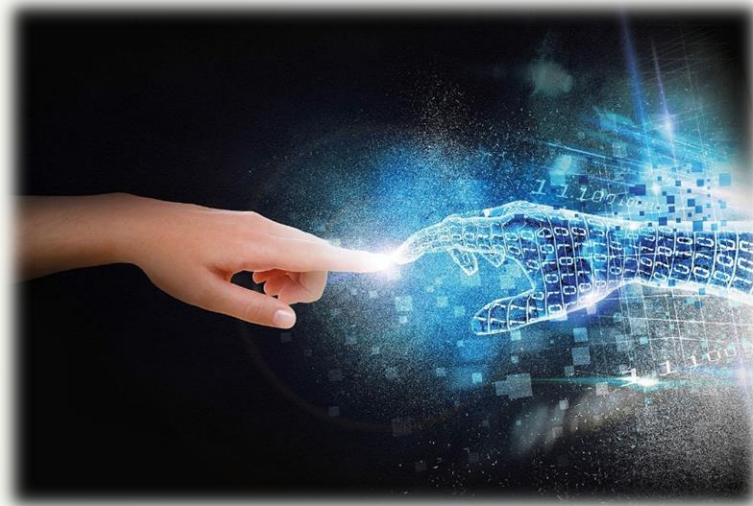


il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR)



Relatore **Avv. Giulio Marchesi**

BERGAMO (BG) Via T. Tasso - SALA VITERBI DELLA PROVINCIA

25 settembre 2018

Il problema del trattamento dei dati



IL LUNEDÌ NERO DI ZUCKERBERG

Facebook crolla a Wall Street (-7%) sullo scandalo Cambridge

Uber, rubati i dati di milioni di clienti: la multinazionale ha taciuto e pagato un riscatto

Centomila dollari agli hacker che nel 2016 hanno piratato nomi, email, numeri di telefono



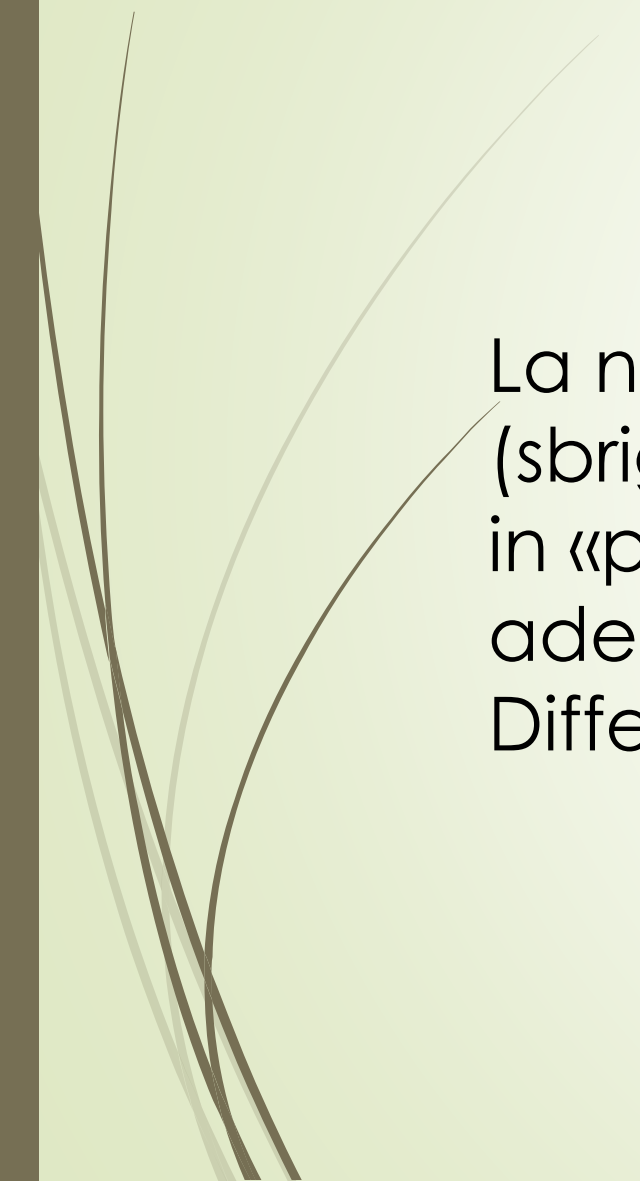
Il problema del trattamento dei dati

Altro che privacy, ecco come un compratore di dati scopre la vostra identità

Due ricercatori hanno comprato dei pacchetti di “dati di navigazione in forma anonima” per dimostrare quanto è facile risalire alle informazioni degli utenti



Il problema del trattamento dei dati



La normativa sul trattamento dei dati (sbrigativamente ed erroneamente condensata in «privacy») ha finito per essere un sottovalutato adempimento formale, disatteso dai più. Differente nei vari Paesi UE.



La soluzione: il nuovo regolamento UE 679/2016

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.





► **Per l'interpretazione del Regolamento c.d. «Privacy» sono importanti i «considerando» (ben 173!) che fanno parte della premessa.**


► I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.


➤ **Per i trattamenti di dati si va oltre il principio di stabilimento**


- La “privacy UE” riguarda anche imprese extra-comunitarie che forniscano beni o servizi o che monitorino i comportamenti e/o le abitudini di vita degli interessati. E' attuata una significativa espansione del campo di applicazione delle norme che sembra puntare ad una tutela più ampia e sistematica delle persone. Ognuno dei 3 commi che compongono l'art. 3 contiene un distinto 'criterio' di definizione dell'ambito.
- **1. quando il titolare o il responsabile del trattamento è stabilito nell'Unione**, il Regolamento si applica ai trattamenti anche se i medesimi sono effettuati al di fuori dell'UE;
- **2. se il titolare o il responsabile non è stabilito nell'Unione**, è sufficiente per l'applicazione che si trovino nell'Unione gli interessati i cui dati personali siano oggetto di trattamento e i medesimi interessati siano destinatari di offerte di beni o prestazioni di servizi, indipendentemente dall'obbligatorietà del pagamento, ovvero quando il titolare o il responsabile sottopongano il comportamento degli stessi (che abbia luogo dentro l'UE) ad azioni di monitoraggio;
- **3. infine, nel caso di titolare stabilito al di fuori dell'Unione**, si applica il Regolamento quando il medesimo è stabilito in un luogo soggetto al diritto di uno Stato UE in virtù del diritto internazionale pubblico.


- 
- **Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione dei dati personali (*data breach*).**


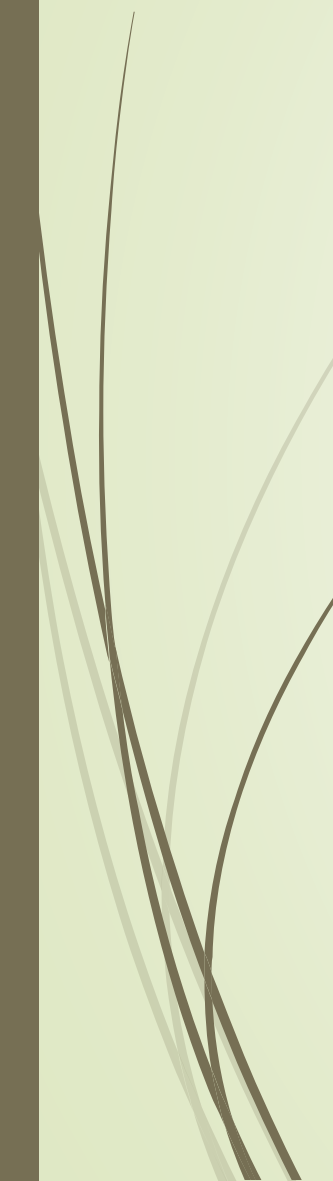
- 
- ▶ La prima differenza concerne la collocazione delle norme: nella Direttiva 95/46/CE gli artt. 10 e 11 sono nella sezione IV (“Informazione della persona interessata”) del Capo II (“Condizioni generali di liceità dei trattamenti di dati personali”), così come nel Testo Unico italiano (D. Lgs. 196/2003) l'art. 13 è all'interno del Titolo III (“Regole generali per il trattamento dei dati”).
 - ▶ Dunque il Regolamento compie un salto di qualità nel momento in cui inquadra gli artt. 13 e 14 nel Capo III che verte sui “diritti dell'interessato”. E' un mutamento di ottica non secondario: **da condizione di liceità o regola di un trattamento** – che rileva anzitutto come adempimento del titolare – **si passa a qualificare l'informativa come diritto dell'interessato**; trattandosi, per l'esattezza, del primo e fondamentale diritto dell'interessato, cui fanno seguito il diritto all'accesso (art. 15), alla rettifica (art. 16), alla cancellazione (art. 17), alla limitazione (art. 18), alla portabilità (art. 20), all'opposizione (art. 21).

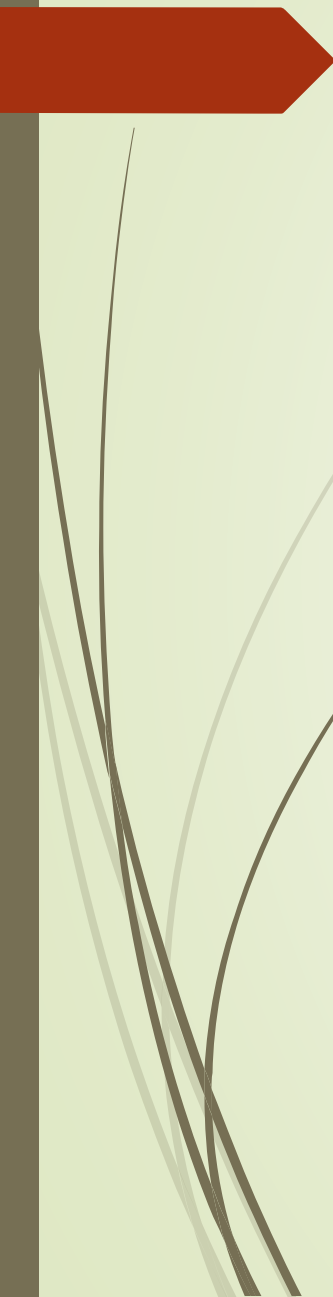
- 
- ▶ La seconda novità è che **l'art. 13, comma 1, del Testo Unico italiano richiedeva che l'interessato sia “previamente” informato, mentre gli artt. 13 e 14 del Regolamento fanno riferimento alla fornitura dell'informativa “nel momento in cui i dati personali sono ottenuti”**.
 - ▶ Sembra introdotto un diverso limite temporale, per cui è sufficiente che l'informativa sia contestuale – ancorché immediatamente successiva - alla raccolta. Con ciò si intende significare che l'art. 13 del Testo Unico italiano aveva e ha introdotto un termine più stringente di quanto richiesto dalla stessa Direttiva 95/46/CE e che non è ininfluente sotto il profilo della consapevolezza dell'interessato, anche e a maggior ragione a prescindere dall'ipotesi in cui l'interessato sia chiamato ad esprimere il proprio consenso.


- 
- La terza novità è la **codificazione del criterio del “linguaggio semplice e chiaro”**
 - mediante il quale il titolare deve rendere all'interessato tutte le informazioni e le comunicazioni. Si tratta di requisito indicato all'art. 12 (“Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato”) e significativamente presente nei considerando 39 e 58, il primo dei quali è particolarmente rilevante da un punto di vista ermeneutico.


- 
- (39) Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto.
 - Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.


- 
- ▶ La quarta differenza risiede nel **contenuto dell'informativa, che il Regolamento complessivamente amplia rendendola (un po') più ricca di informazioni ma anche più onerosa per il titolare che deve redigerla.**
 - ▶ Anzitutto c'è una bi-partizione nel nuovo art. 13 che è solo apparente, poiché il primo e il secondo gruppo di informazioni debbono rendersi nel momento in cui i dati sono ottenuti e pertanto una e una sola è l'informativa da comunicare all'interessato.
 - ▶ La gran parte delle 'aggiunte' dell'art. 13 del Regolamento dopo una prima lettura si lascia ricondurre ad alcuni dei sei requisiti dell'art. 13 dell'attuale Testo Unico.


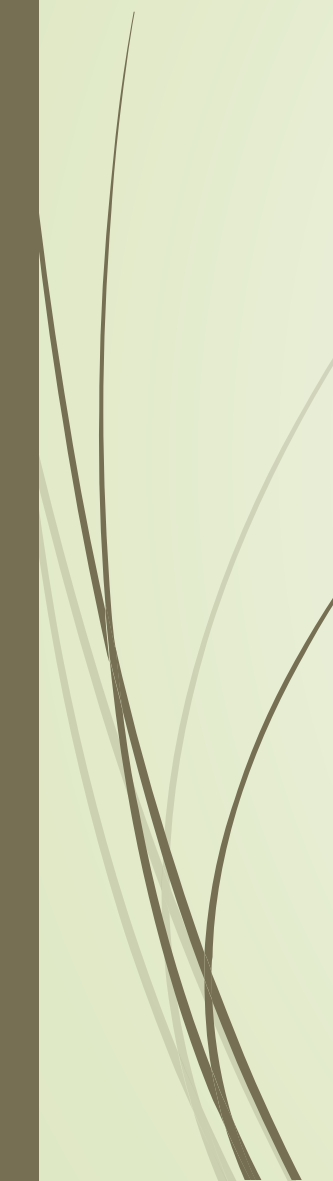
- 
- L'informativa diventa sempre di più uno strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti.
 - Per facilitare la comprensione dei contenuti, nell'informativa si potrà fare ricorso anche a icone, identiche in tutta l'Unione europea.
 - Gli interessati dovranno sapere se i loro dati sono trasmessi al di fuori dell'Ue e con quali garanzie; così come dovranno sapere che hanno il diritto di revocare il consenso a determinati trattamenti, come quelli a fini di marketing diretto.
- 


- 
- ▶ Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web).
 - ▶ Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito». Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate.
 - ▶ Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.
 - ▶ I fornitori di servizi Internet e i social media, dovranno richiedere il consenso ai genitori o a chi esercita la potestà genitoriale per trattare i dati personali dei minori di 16 anni.


- 
- ▶ Le decisioni che producono effetti giuridici (come, la concessione di un prestito) non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio, la profilazione).
 - ▶ Faranno eccezione i casi in cui l'interessato abbia rilasciato un consenso esplicito al trattamento automatizzato dei suoi dati, oppure questo tipo di trattamento risulti strettamente necessario per la definizione di un contratto o avvenga in base a specifici obblighi di legge.
 - ▶ In ogni caso, sono previste garanzie per gli interessati, come il diritto di opporsi alla decisione adottata sulla base di un trattamento automatizzato o il diritto di ottenere anche l'intervento umano rispetto alla decisione stessa.
 - ▶ Se il trattamento è finalizzato ad attività di marketing diretto, l'interessato ha sempre il diritto di opporsi alla profilazione.


- 
- Grazie all'introduzione del cosiddetto «diritto all'oblio», gli interessati potranno ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento qualora ricorrano alcune condizioni previste dal Regolamento: se i dati sono trattati solo sulla base del consenso; se i dati non sono più necessari per gli scopi rispetto ai quali sono stati raccolti; se i dati sono trattati illecitamente; oppure se l'interessato si oppone legittimamente al loro trattamento.
 - A questo diritto si accompagna l'obbligo per il titolare del trattamento che ha pubblicato i dati di comunicare la richiesta di cancellazione a chiunque li stia trattando, nei limiti di quanto tecnicamente possibile.


- 
- Il Regolamento introduce il diritto alla «portabilità» dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.
 - Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati.
 - Ci saranno però alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.


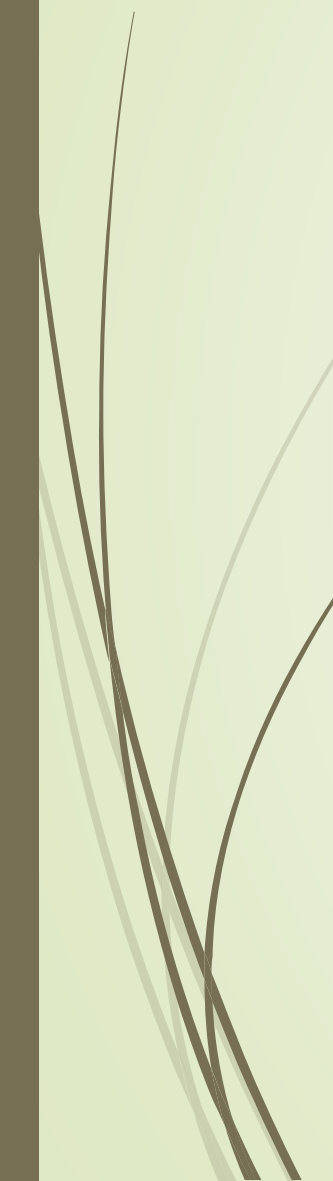
- 
- ▶ Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.
 - ▶ Come avviene già oggi, in mancanza di un riconoscimento di adeguatezza da parte della Commissione europea, i titolari potranno utilizzare per il trasferimento specifiche garanzie contrattuali, per le quali il Regolamento prevede norme dettagliate e vincolanti.
- 


- 
- ▶ 'sticky regulation', “regolazione che resta 'attaccata' ai dati al fine di tutelarli a seguito di qualsiasi successivo ed ulteriore trasferimento
 - ▶ *“I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. **È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. (...)”***


- 
- ▶ In assenza di garanzie contrattuali o riconoscimenti di adeguatezza, i dati potranno essere trasferiti solo con il consenso esplicito dell'interessato, oppure qualora ricorrano particolari condizioni (ad esempio, quando il trasferimento è indispensabile per rispettare specifici obblighi contrattuali, per importanti motivi di interesse pubblico, per esercitare o difendere un diritto in sede giudiziaria, ecc.).
 - ▶ Il trasferimento o la comunicazione di dati personali di un cittadino dell'Ue ad autorità giudiziarie o amministrative di Paesi terzi potranno avvenire solo sulla base di accordi internazionali di mutua assistenza giudiziaria o attraverso strumenti analoghi.


- 
- Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati. Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.
 - Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine, ecc.); oppure se dimostrerà di avere adottato misure di sicurezza (come la cifratura) a tutela dei dati violati; oppure, infine, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato (ad esempio, se il numero delle persone coinvolte è elevato). In questo ultimo caso, è comunque richiesta una comunicazione pubblica o adatta a raggiungere quanti più interessati possibile (ad esempio, tramite un'inserzione su un quotidiano o una comunicazione sul sito web del titolare).

- 
- ▶ Imprese ed enti avranno più responsabilità, ma potranno beneficiare di semplificazioni. In caso di inosservanza delle regole sono previste sanzioni, anche elevate.
 - ▶ Il Regolamento è direttamente applicabile e vincolante in tutti gli Stati membri dell'Unione europea e non richiede una legge di recepimento nazionale.
 - ▶ Inoltre, si applica integralmente alle imprese situate fuori dall'Unione europea che offrono servizi o prodotti a persone che si trovano nel territorio dell'Unione europea. Tutte le aziende, ovunque stabilite, dovranno quindi rispettare le regole fissate nell'Ue.

- 
- Fra le principali novità del Regolamento c'è il cosiddetto «sportello unico» (*one stop shop*), che semplificherà la gestione dei trattamenti e garantirà un approccio uniforme.
 - Salvo casi specifici, le imprese stabilite in più Stati membri o che offrono prodotti e servizi in vari Paesi dell'Ue, per risolvere possibili problematiche sull'applicazione e il rispetto del Regolamento potranno rivolgersi ad un solo interlocutore: cioè all'Autorità di protezione dei dati del Paese dove si trova il loro stabilimento principale.
- 


- 
- Il Regolamento promuove la responsabilizzazione (*accountability*) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.


- 
- ▶ Il principio-chiave è «*privacy by design*», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.
 - ▶ Ad esempio, è previsto l'obbligo di effettuare valutazioni di impatto prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, consultando l'Autorità di protezione dei dati in caso di dubbi.
 - ▶ Viene inoltre introdotta la figura del «Responsabile della protezione dei dati» (*Data Protection Officer* o DPO), incaricato di assicurare una gestione corretta dei dati personali nelle imprese e negli enti.

- 
- Novità tra le più pubblicizzate del Regolamento europeo, il Responsabile per la Protezione dei Dati (**Data Protection Officer**) - figura disciplinata dagli artt. 37, 38 e 39 - fa la sua entrata in scena nel nostro ordinamento giuridico.
 - “Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
 - a) **il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
 - b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**; oppure
 - c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.”

► *Articolo 38* **Posizione del responsabile della protezione dei dati**

- 1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. 4.5.2016 L 119/55 Gazzetta ufficiale dell'Unione europea IT
- 2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
- 3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
- 4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
- 5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
- 6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

- 
- ▶ Il Regolamento promuove il ricorso a codici di condotta da parte di associazioni di categoria e altri soggetti, sottoposti all'approvazione dell'Autorità nazionale di protezione dei dati ed eventualmente della Commissione europea (nel caso dell'approvazione da parte della Commissione il codice di condotta avrà applicazione nell'intera Ue).
 - ▶ Il titolare potrà far certificare i propri trattamenti, in misura parziale o totale, anche ai fini di trasferimenti di dati in Paesi terzi. La certificazione potrà essere rilasciata da un soggetto abilitato oppure dall'Autorità di protezione dei dati.
 - ▶ L'adesione ai codici di condotta e la certificazione del trattamento saranno elementi di cui l'Autorità dovrà tenere conto, per esempio, nell'applicare eventuali sanzioni o nell'analizzare la correttezza di una valutazione di impatto effettuata dal titolare.

- 
- ▶ Il 23 gennaio 2017 il Consiglio d'Europa ha pubblicato alcune **Linee Guida per la protezione degli individui con riguardo al trattamento dei dati personali nell'era dei Big Data** (*"Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data"*), nelle quali sono precisati alcuni dei principi e delle disposizioni vigenti in materia di protezione dei dati personali in relazione ai rischi specifici che l'utilizzo dei Big Data può comportare.
 - ▶ I valori e i diritti coinvolti impongono l'adozione di un approccio preventivo e il Consiglio d'Europa richiama il procedimento di analisi del rischio, già fatto proprio dal Regolamento generale per la protezione dei dati personali (Regolamento 679/2016/UE del Parlamento europeo e del Consiglio del 27 aprile 2016), specificando che il rischio analizzato non concerne soltanto il possibile rischio per il singolo individuo ma deve altresì estendersi ai rischi per la collettività e deve considerare l'impatto legale, sociale ed etico dell'utilizzo dei Big Data, con particolare attenzione ai principi di uguaglianza e non discriminazione.

➤ Ma in concreto cosa devono fare gli avvocati?

➤ Rispettare i principi di cui all'art. 5, per cui i dati personali sono:

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

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

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

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

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

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

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

► Ma in concreto cosa devono fare gli avvocati?

► **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;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

► Ma in concreto cosa devono fare gli avvocati?

- Ridefinire tipo e consistenza dei dati trattati, indicando le finalità e la necessità
- Definire i ruoli del titolare del trattamento dei dati (in ipotesi Legale rappresentante), individuare ruoli e funzioni di eventuali “responsabili” per il trattamento dei dati e, opportuno ma non obbligatorio, delegare specifiche funzioni agli “incaricati”.
- Eventualmente, o necessariamente ricorrendone i presupposti, nominare un Responsabile della Protezione dei Dati (RPD o in inglese DPO Data Protection Officer), una figura autonoma e con potere decisionale e di spesa che si rapporta solo con i vertici dell’Ente.
- Reformulare la modulistica relativa alle informative, ai consensi, ai reclami, al diritto di accesso ai dati, privilegiando le modalità telematiche.
- Adottare, ove previsto, il Registro delle attività di trattamento, preferibilmente in forma elettronica.
- Rivedere e/o adottare misure per la sicurezza dei dati, in specie per il sistema informatico, con strategie di archiviazione, conservazione a norma e disaster recovery.
- Effettuare una Valutazione di impatto sulla protezione dei dati (assessment – art. 35 GDPR)
- Adottare codici di condotta (e/o certificazioni, quando saranno disponibili e definite le relative autorità).

Il registro del trattamento dei dati

- Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
 - a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
 - b) le finalità del trattamento;
 - c) una descrizione delle categorie di interessati e delle categorie di dati personali;
 - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
 - e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
 - f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
 - g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.



Il registro del trattamento dei dati

- Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

► La comunicazione delle violazioni

- 1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

- 3. La notifica di cui al paragrafo 1 deve almeno:
 - a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
 - b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
 - c) descrivere le probabili conseguenze della violazione dei dati personali;
 - d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

► La comunicazione delle violazioni

- 1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
- 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
- 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
 - a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;



► La valutazione d'impatto (assessment)

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



➤ **CryptoWall: l'evoluzione di CryptoLocker**

- Il panorama italiano dei ransomware si è dotato di un nuovo componente, **CryptoWall**, evoluzione del più famoso CryptoLocker, recentemente messo in ginocchio da un'operazione coordinata da varie polizie internazionali.
- Attivo negli Stati Uniti fin da aprile 2014, con le prime vittime illustri nel maggio 2014, **ora sembra aver preso di mira gli utenti italiani**, complice anche il suo inserimento nell'exploit kit RIG.
Nell'ultima settimana sono molte le segnalazioni di infezioni che richiedono il **pagamento di un riscatto mediante bitcoin** da depositare in un sito raggiungibile solamente attraverso la rete TOR.



1. You should register Bitcoin wallet ([click here for more information with pictures](#))

2. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

- [localbitcoins.com](#) - Buy Bitcoins with Western Union
- [Coin.mg](#) - Recommended for fast, simple service. Takes Credit Card, Debit Card, ACH, Wire
- [LocalBitcoins.com](#) - Service allows you to search for people in your community willing to sell bitcoins to you directly.
- [colntr.com](#) - Another fast way to buy bitcoins
- [bitquick.co](#) - Buy Bitcoins Instantly for Cash
- [How to Buy Bitcoins](#) - An international directory of bitcoin exchanges.
- [Cash Into Coins](#) - Bitcoin for cash.
- [CoinJar](#) - CoinJar allows direct bitcoin purchases on their site.
- [anxpro.com](#)
- [bitfurious.com](#)
- [ZipZap](#) - ZipZap is a global cash payment network enabling consumers to pay for digital currency.

3. Send 1.25 BTC to Bitcoin address: [1MyhRLoPBjxcQ9h0c27oYHjDSdzDkEXjs](#) [Get QR code](#)

4. Enter the Transaction ID and select amount:

Note: Transaction ID - you can find in detailed info about transaction you made.
(example 44214e1ca56e039308ddb929c40b034119a27c42107f5c03e2aa00114c4d102)

5. Please check the payment information and click "PAY".

PAY



➤ CryptoWall: l'evoluzione di CryptoLocker

- Il metodo di infezione risulta essere una mail contenente un allegato fraudolento, nella maggior parte dei casi un file che appare come PDF, contenente codice malevolo che **scansiona l'intero filesystem**, comprese le condivisioni di rete, **e ne cripta il contenuto**.

Una prima analisi sui valori entropici e sulla struttura del file criptato sembra suggerire l'utilizzo di un cifrario RSA con chiavi a 2048 bit, che elimina completamente la possibilità di attaccare la cifratura mediante tecniche di bruteforce.



► *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.




► **Articolo 83**


Condizioni generali per infliggere sanzioni amministrative pecuniarie (C148, C150-C152)


1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.


- 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;

- 
- **Dal 19 settembre il d.lvo 101/2018 è entrato in vigore e deve essere applicato e fatto applicare come una legge dell'ordinamento italiano.**
 - E' finito il periodo di *vacatio legis* che, non essendovi alcuna previsione specifica né nella legge di delega 25 ottobre 2017 n.163, né nel decreto legislativo delegato è ovviamente l'ordinario periodo previsto dall'art.73 della Costituzione.

- 
- L'intera normativa italiana in materia di tutela dei dati personali va letta, interpretata e applicata in un quadro estremamente complesso che comprende il GDPR e il Codice oggetto del d.lvo 196 del 2003 come novellato dal d.lvo 101 del 2018.
 - Non esiste alcun periodo *soft* di applicazione della nuova normativa, né da parte della Autorità Garante né da parte di tutti coloro ai quali spetta osservarla e farla osservare. Il periodo di otto mesi dall'entrata in vigore del d.lvo n.101 rileva unicamente ai fini dei criteri che l'Autorità Garante deve tener presente nel definire **le eventuali sanzioni pecuniarie** da applicare per le violazioni alle disposizioni contenute nel decreto, e anche questo, come precisa l'art. 22 comma 13, unicamente "nei limiti in cui risulti compatibile col Regolamento (UE) 2016/679".

- 
- Tutta la normativa italiana in materia, sia quella contenuta nel d.lvo n. 196 del 2003 e non abrogata o modificata dal d.lvo n. 101 del 2018, sia quella contenuta in questo ultimo, nuovo, decreto, deve essere interpretata e applicata alla luce del GDPR e in conformità alle sue norme.

- 
- All'art. 22, comma 13 del D.lgs. 101/2018 si legge: “Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie.”
 - Ciò sta a significare che il Garante per i primi otto mesi sarà più “clemente” nell'erogare le sanzioni, operando una valutazione di tanti fattori, come peraltro era stato già indicato nelle Linee guida del Comitato europeo (ex WP29) del 3 ottobre 2017.



Grazie per l'attenzione