Studio Legale Tamos & Partners
www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
lorenzo.tamos@avvocatinteam.com – tel. mobile 339-6438001

I DATI PERSONALI DEGLI INDIVIDUI E LA LECITA CIRCOLAZIONE DEGLI STESSI

IL REGOLAMENTO UE N. 679/2016

COME ADEGUARSI

E PERCHE' FARLO, AL DI LA' DELLE SANZIONI

Studio Legale Tamos & Partners
www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
lorenzo.tamos@avvocatinteam.com – tel. mobile 339-6438001

1. PREMESSE E RAGIONI DI FONDO DELL'ADEGUAMENTO

Se la **libertà** e la **salute** sono concetti storicamente **percepiti** come diritti fondamentali degli uomini, la **protezione dei dati** personali è un valore posto in rilievo **solo in tempi recenti** sebbene non siano mancati **eventi terribili** il cui verificarsi è dipeso dall'assenza di protezione delle informazioni riguardanti le persone, soprattutto di quelle legate al pensiero culturale, politico o religioso delle stesse.

Non è dunque un caso che **Billy Graham** (scrittore statunitense[1]), insieme a molte altre voci meno note, già negli anni ottanta abbia eloquentemente affermato che <<**solo una volta che hai perso la tua "privacy", ti accorgi di aver perso una "cosa" estremamente preziosa**>>.

Da questa considerazione generale di "**preziosità**" muove la nuova regolamentazione europea visto che la **libera circolazione dei dati personali** degli individui è da tempo diventata "cosa" altrettanto preziosa, e non solo in senso strettamente economico.

Ma innanzitutto occorre operare un distinguo: difatti **non bisogna confondere** il concetto di **"privacy"** con la normativa in materia di **corretto trattamento dei dati**[2]. La prima è un diritto individuale che tutela il singolo nella sua esclusività ed intimità (<<nella sua solitudine>>), il secondo tutela l'individuo oltre la sfera della vita privata attribuendogli (una buona dose di) autonomia decisionale ed il controllo sulla circolazione dei propri dati personali nell'ambito delle relazioni sociali ed economiche che lo riguardano.

I due piani sono molto diversi anche se, a volte, si confondono perché spesso gli uni si intersecano con gli altri[3].

o0o

La circolazione del dato personale quale necessità imprescindibile

L'equazione del **compromesso storico** sulla protezione dei dati rispetto alla loro circolazione, per come ad oggi attuato dall'Unione Europea, è semplice ma non banale: la protezione dei dati personali è direttamente

1 Billy Graham (1918-2018) insignito della medaglia delle libertà nel 1983.

2 Il diritto alla protezione dei dati personali è ad esempio sancito dall'**art. 12** della Dichiarazione universale dei diritti dell'uomo delle Nazioni Unite. Nel **1948**, tale Dichiarazione ha, per la "prima volta", previsto tale diritto. Il diritto alla protezione dei dati è sancito anche nella Carta dei diritti dell'Unione europea (Carta di Nizza) del 2000. Oggi il Reg. 679/2016 lo proclama come diritto fondamentale autonomo che, però, deve coesistere con altri diritti quali, in primo luogo, il diritto di poter far circolare i dati (forse da considerarsi addirittura "primario" rispetto alla protezione), il diritto di libertà di stampa e di manifestazione del pensiero.

3 Per metaforico esempio confondere i due concetti sarebbe come sostenere che il diritto alla vita dell'individuo, nelle sue più ampie declinazioni, sia la stessa cosa del diritto di ricevere cure sanitarie adeguate per il caso di una malattia.

proporzionale alla sempre **maggiore circolazione sociale** degli stessi[4].

Recita infatti il 4° considerando del Regolamento 679/2016 che <<il **diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta**, ma va considerato alla luce della sua **funziona sociale** e **va contemperato con altri diritti fondamentali**>>.

Ed ancora il 6° considerando del Regolamento afferma che <<la tecnologia ha trasformato l'economia e le relazioni sociali e **dovrebbe facilitare ancora di più la libera circolazione dei dati personali** all'interno dell'Unione **ed il loro trasferimento verso paesi terzi** e organizzazioni internazionali, **garantendo al tempo stesso un elevato livello di protezione dei dati personali**>>.

Citando quindi chi il nostro mondo ha contributo a cambiare radicalmente, è possibile ritenere ben vero come <<**storicamente, "la privacy" era quasi implicita**, perché era difficile trovare e raccogliere informazioni, **oggi, invece**, nel mondo digitale, che si tratti di telecamere o satelliti o semplicemente di un clic sul computer, **abbiamo bisogno di avere norme più esplicite** non solo per i governi, ma anche per le imprese private[5]>> (**Bill Gates**, ex imprenditore statunitense).

E così oggi è, o almeno dovrebbe essere, essendo **impensabile poter organizzare un'attività d'impresa facendo meno dei dati delle persone**, ovvero poter credere di precludersene il trattamento, specie al di sotto di certi **livelli di flusso** "fisiologico", implicito al concetto stesso d'azienda funzionale sul mercato nazionale ed internazionale[6].

Basti valutare la sempre più **vasta conservazione di dati c.d. "comuni**" in un qualsiasi **computer portatile aziendale** per rendersi conto di tale **necessità** di organizzazione e trattamento e, quindi, di protezione.

---

4 Nel 10° cons. del Reg. si legge: <<al fine di assicurare un livello coerente ed elevato di **protezione delle persone** fisiche **e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'unione**, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati **dovrebbero essere equivalente in tutti gli Stati** membri>>.

5 Verrebbe qui spontaneo aggiungere <<*soprattutto per le grandi imprese private nel campo della c.d. info-sfera* [o **frontiera del mondo informatico e digitale**]>>.

6 Non a caso la Convenzione di Strasburgo del **1981**, detta <<**Convenzione 108>>** del Consiglio d'Europa, è stato ed è uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato di dati personali. Essa ad oggi è l'unico strumento giuridico vincolante a livello internazionale in tale materia a cui possono aderire Stati non membri del Consiglio d'Europa. Questa convenzione nasce dall'esigenza di **tutela** a seguito del proliferare di tecnologie dell'informazione e comunicazione **a partire dagli anni 60**. Essa si applica a tutti i trattamenti di dati personali effettuati nel settore privato e pubblico, anche ai trattamenti effettuati da polizia e autorità giudiziaria. La normativa vuole proteggere gli individui da abusi e regolamentare i flussi transnazionali dei dati traendo inspirazione dall'**art. 8** della Convenzione europea dei diritti dell'uomo.

Ma la normativa in commento trova vera ragione d'essere nel tentativo del legislatore europeo di **regolamentare** il potere di trattamento esercitato soprattutto negli ultimi **tre decenni** da alcuni **grandi players economici globali** (poiché) diventati **potentissimi** ed **incontrollabili** nella raccolta di dati "appartenenti" a più della metà degli individui viventi e non a livello globale. Si tratta di quantitativi di informazioni davvero **impressionanti** ed **importantissimi** sia per le società private che per i governi che quei grandi players mondiali stanno tentando di arginare.

E **siamo solo all'inizio di un periodo storico** che, sotto certi aspetti, è **molto simile** a quello della prima **rivoluzione industriale** dei due secoli scorsi in cui il diritto alla salute, alla prevenzione, al riposo degli individui ha, per troppo tempo, ceduto il passo alle sole esigenze della produzione massiva: il vero prezzo che stiamo pagando e che, metaforicamente, non riusciremo del tutto a saldare quale conseguenza di questo fisiologico disinteresse storico, è oggi sotto gli occhi di tutti e non è affatto tranquillizzante.

Viene da chiedersi, quindi, quali **reali chances** (e spinte motivazionali) **avranno i governi nazionali di proteggere** davvero i dati (i diritti fondamentali) degli individui, soprattutto a fronte di interessi economici dirompenti e di una **regolamentazione frammentata** a livello mondiale: sarà con tutta probabilità più facile che la risposta reale e concreta a queste esigenze di protezione arrivi dal settore privato in forza della sempre maggiore "domanda" dell'utenza (e non solo dai governi).

Se, infatti, abbiamo assistito ad una vera e propria incontrollata "invasione" di prodotti (**beni materiali**) provenienti da paesi lontani non sempre realizzati nel rispetto dei più basilari diritti degli uomini, sarà ancora più difficile credere che le normative di salvaguardia dei dati delle persone (quali preziosi **beni immateriali**) possano davvero produrre tutti gli ambiziosi effetti protettivi sperati/evocati dalla normativa europea.

o0o

La tutela del dato è un diritto fondamentale dell'individuo

Ecco perché l'ambizioso **7° considerando** del Regolamento sancisce – in ritardo rispetto ad una realtà già evolutasi da anni – che <<tale **evoluzione** richiede **un quadro più solido e coerente in materia di protezione dei dati nell'Unione**, affiancato da efficaci misure di attuazione, dato l'importanza di creare il **clima di fiducia** che consentirà lo sviluppo [alias: circolazione del dato] dell'economia digitale in tutto il mercato interno.

E' opportuno che **le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata** tanto per le **persone fisiche** quanto per gli **operatori economici e le autorità pubbliche**>>.

Del resto, essendo la <<protezione delle persone fisiche, con riguardo

al trattamento dei dati di carattere personale, un **diritto fondamentale**>>[7] questo diritto è da porsi senza dubbio a base <<**del progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel marcato interno e al benessere delle persone fisiche**>> (cfr. 2° consid. del Reg.).

o0o

Lo stretto connubio tra circolazione del dato e sua protezione

A livello aziendale, come ad esempio già accaduto per la sicurezza e la prevenzione della salute dei lavoratori, nonché per la tutela dell'ambiente in generale, gli operatori economici europei (specie quelli più avveduti) sposteranno parte significativa delle proprie risorse organizzative verso la migliore protezione possibile del dato personale.

Questo accadrà non solo per timore dal pesante apparato sanzionatorio previsto ma perché le aziende si renderanno conto che ciò costituisce un **presupposto** ed un forte **vantaggio competitivo** oltre che il modo giusto di garantire ai propri collaboratori, agli utenti ed alla clientela in generale la protezione di un diritto fondamentale dell'individuo[8].

Si tratta di un **valore che verrà sempre più percepito come un diritto di base da parte di ogni individuo** che, perciò, lo vorrà esercitare in modo informato, trasparente, protettivo e consapevole, soprattutto laddove "dato in custodia" ad altri.

o0o

Il rispetto della normativa UE in azienda: un punto di forza

In questo nuovo scenario anche le imprese meno grandi (o meno informatizzate) potranno certamente **competere** con i "colossi" multinazionali cercando quanto meno di (predisporsi per) **attrarre clientela** e nuovi **utenti pure** in ragione dell'applicazione della normativa in oggetto. Tutto ciò è del resto già accaduto per la produzione c.d. eco compatibile che, invero, ha fatto in molti casi la vera differenza in termini di buoni risultati di mercato e di ampliamento dello stesso.

Insomma, anche grazie alla normativa europea, una **nuova sfida** è posta perché – **per chi ne saprà vedere i vantaggi** – non si tratterà di offrire un pacchetto preconfezionato di misure di trattamento a protezione dei dati per evitare le sanzioni, bensì, garantire in concreto una procedura a misura aziendale da rappresentare all'esterno come un **valore aggiunto** su cui la

7 **1° considerando del Reg**. e **art. 8**, **par. 1** della **Carta dei diritti fondamentali dell'unione europea**, art. 16, par. 1 del trattato sul funzionamento dell'Unione.

8 E' interessante il parallelismo d'esempio offerto in proposito dal Prof. Ugo Mattei (giurista contemporaneo) tra la **frontiera del vecchio mondo** – ed il saccheggio incontrollato ivi perpetrato dai coloni del tempo – con la **nuova frontiera della c.d. "info-sfera"** (il mondo digitale) in cui, secondo Mattei, si è verificato negli ultimi decenni una sorta di simile incontrollato saccheggio a danno dei dati personali degli individui.

clientela e l'utenza potrà **fare affidamento**.

Per poter raccogliere (e vincere) la sfida ogni operatore economico dovrebbe, però, in primo luogo, porsi e rispondere con sincerità alle seguenti domande:

1. raccolgo **troppi dati** personali rispetto agli scopi ed obiettivi aziendali?
2. Potrei raggiungere gli stessi risultati anche con **meno dati**?
3. Ho individuato lo scopo e la **finalità** reale della raccolta dei dati?
4. Ho **informato** delle mie finalità i soggetti a cui i dati si riferiscono?
5. Questi **soggetti** sanno come vengono trattati i loro dati in azienda?
6. Ho una adeguata **procedura** per la verifica dell'esattezza ed aggiornamento dei dati?
7. Che **misure** e procedure di sicurezza, di backup e di trasferimento ho in azienda rispetto ai dati che tratto?
8. Ho idea di **quanto tempo** i dati vangano trattati ed ho delle procedure che mi permettano di trattarli solo per il tempo "strettamente" necessario al raggiungimento degli scopi ed esigenze aziendali?
9. Sono in grado di **garantire agli interessati** il diritto di accesso, di rettifica, di cancellazione e portabilità nei tempi prefissati dalla normativa?

Se a queste domande non si è in grado di rispondere affermativamente bisogna senza dubbio prendere in seria considerazione la normativa UE ed adeguarsi rapidamente ai precetti posti dalla stessa.

o0o

2 IL REGOLAMENTO UE 2016/679

Il Regolamento UE 2016/679 (conosciuto anche con l'acronimo "**GDPR**": <<**G**eneral **D**ata **P**rotection **R**egulation>>) ha il dichiarato scopo di fortificare in modo omogeneo la protezione dei dati personali dei **cittadini e residenti** (persone fisiche) dell'Unione Europea sia all'interno che all'esterno dei confini territoriali dell'Unione stessa, al fine di **unificare le legislazioni** degli Stati membri sotto un'unica regolamentazione sovranazionale.

Il dettagliato Regolamento, difatti, a far data dal 25 maggio 2018 (art. 99), è **direttamente applicabile** e **prevalente** in tutti gli stati dell'Unione Europea **senza alcuna necessità da parte di questi di adottare normative nazionali di recepimento**.

Con l'inizio dell'applicazione del Regolamento si potranno, perciò, in buona sostanza, verificare due situazioni:

> **(A)** o la normativa europea **disapplicherà** quella nazionale ad eccezione della regolamentazione domestica relativa agli ambiti c.d. residuali (o di "coordinamento") e, quindi, gli operatori economici nei

vari Stati dovranno autonomamente capire cosa della normativa nazionale resterà ancora in vigore; ovvero

(B) i singoli Stati membri, per mezzo di **nuove leggi nazionali**, **indicheranno** (più o meno) esattamente cosa della "vecchia" normativa domestica in materia di privacy resterà ancora in vigore, sempre nella misura in cui essa sarà compatibile con la legislazione introdotta dal Regolamento UE.

L'Italia ha recepito i principi europei per mezzo dell'art. 13 della L. n. 163/2017, entrata in vigore il 21/11/2017, che ha attribuito al Governo la delega ad adottare (entro 6 mesi) uno o più provvedimenti rivolti ad abrogare il Dlgs n. 196/2003, regolare i poteri del Garante e adeguare il regime sanzionatorio (penale ed amministrativo) alle disposizioni del Regolamento 679/2016[9].

o0o

Alcuni passaggi legislativi ed insiemi normativi

Da ricordare che il **Regolamento UE** 679/2016 fa parte di un c.d. "**pacchetto protezione dati**" approvato dal Parlamento Europeo il 14/04/2016 e contenente pure la <<**Direttiva UE 2016/680** relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzioni di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la decisione quadro 2008/977/GAI del Consiglio>>.

Sia il **Regolamento** che la detta **Direttiva** sono stati pubblicati nella Gazzetta Ufficiale dell'Unione Europea il **4 maggio 2016** ed il GDPR, contrariamente alla percezione che i più ad oggi hanno, è **già entrato in vigore** il **24 maggio 2016**, sebbene la sua **applicabilità** sia stata fatta decorrere a **far data dal 25 maggio 2018** con contestuale abrogazione della (al tempo non direttamente applicabile) direttiva 95/46/CE[10].

La suddetta **Direttiva UE 2016/680**, entrata in vigore il 5 maggio 2016, a differenza del Regolamento, **non è direttamente applicabile** tale quale e, dunque, pone l'obbligo del suo recepimento a tutti gli Stati membri attraverso le legislazioni nazionali che i detti Stati devono pertanto emanare entro i due anni successivi e, quindi, entro il **6 maggio 2018**[11].

9 Con Comunicato del Consiglio dei Ministri **n. 75 del 21/03/2018** è stato confermato che il Dlgs n. 196/2003 dal 25/05/2018 verrà (tutto?) abrogato e che un nuovo decreto armonizzerà l'ordinamento interno alla nuova disciplina europea. Un primo **schema di decreto** (composto da un centinaio di articoli) è stato approvato dal Consiglio dei Ministri nella prima seduta del 21/03/2018.

10 <<*Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*>>.

11 Si tratta di una **direttiva non "di serie b"** rispetto al Regolamento in quanto, avrà lo scopo di assicurare la protezione dei dati di indagati, testimoni, persone offese

o0o

Ambito di applicazione territoriale e materiale

Da tempo l'Unione Europea si è resa conto che, per la migliore protezioni dei dati personali (quali beni immateriali), più limitata è l'applicazione "territoriale" della inerente normativa è minori saranno le reali possibilità di offrire concreta tutela agli individui a cui quei dati si riferiscono[12].

E' quindi importante sottolineare che la normativa impone la sua applicabilità, in modo espresso, anche solo alla **mera "proiezione" nell'Unione** di una attività che si traduca in semplici offerte di beni e di servizi, indipendente dalla materiale esistenza degli stessi o dalla presenza materiale o immateriale di chi li offre sul territorio dell'Unione. Si tratta quindi di un significativo passo avanti di tipo normativo.

Gli ampliati **ambiti applicativi territoriali** sono stabiliti dall'**art. 3** del Regolamento il quale sancisce che lo stesso si applichi:

1. al trattamento dei dati personali effettuato nell'ambito delle attività di uno **stabilimento**[13] da parte di un titolare o di un responsabile del trattamento **nell'Unione**, **indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione** (C22);
2. al trattamento **dei dati** di interessati che si trovano **nell'Unione**, effettuato da un titolare o da un responsabile del trattamento **che non è stabilito nell'Unione**, **quando** le attività di trattamento riguardano:

   - (a) l'**offerta di beni o la prestazione di servizi** ai suddetti interessati nell'Unione, indipendentemente dall'obbligo di un pagamento dell'interessato;

   - (b) il **monitoraggio** del loro comportamento nella misura in cui abbia luogo all'interno dell'Unione[14];

---

nel corso delle indagini e durante l'esecuzione della pena, nonché atta a facilitare la condivisione di dati tra le autorità giudiziarie dei vari paesi.

12 L'applicazione del Regolamento è decisamente più ampia rispetto alla portata della Direttiva 95/46/CE ed al Codice Privacy nazionale. L'ampliata applicazione dipende anche dalle sentenze della Corte di Giustizia UE (cfr., ad esempio, la sentenza "**Google Spain** 13/05/2014 causa C- 230/14), nonché dal parere n. 8-16/12/2010 del "Gruppo di Lavoro ex art. 29".

13 Inteso come centro decisionale e/o esecutivo di un operatore economico.

14 Oggi, quindi, si guarda **ai soggetti destinatari dei servizi e beni offerti** dall'azienda per stabilire l'assoggettamento alla normativa europea. Anche gli operatori economici che si trovano al di fuori dell'UE ma che tuttavia elaborano dati personali dei residenti nell'UE nel contesto di attività di profilazione dovranno rispettare il GDPR. Il Considerando n. 23 ritiene rilevanti alcuni fattori quali: l'utilizzo di una lingua o di una moneta abitualmente usata in uno o più Stati membri con la possibilità di ordinare beni e servizi in tale altra lingua; la menzione di clienti o utenti che si trovano nell'Unione.

3. al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo **soggetto al diritto di uno Stato membro** in virtù del diritto internazionale pubblico>> (C25).

L'ambito di **applicazione materiale** è ben spiegato dall'**art. 2** del Regolamento ove è stabilito che lo stesso si applica al trattamento di dati personali:

1. interamente o parzialmente **automatizzato** e
2. a quello **non automatizzato** di dati personali ("se") contenuti in un **archivio** o destinati a **figurarvi**[15].

Rimangono esclusi i trattamenti c.d. personali e domestici, quelli effettuati dagli Stati membri per funzioni istituzionali, e quelli di cui al regolamento CE 45/2001 per gli atti istituzionali e giuridici degli organi dell'Unione.

o0o

Le maggiori "innovazioni" apportate dal Regolamento

Se da una parte il Regolamento apporta delle **novità**, poiché sconosciute alla precedente normativa nazionale, dall'altra si limita ad operare una sorta di **restyling** (o "copiatura") di ciò che già era previsto in Europa o in altre nazioni extra UE.

DATO PERSONALE

Partendo dal detto "restyling" il Legislatore Europeo[16] ha, in primo luogo, significativamente dettagliato la definizione di **dato personale** di cui all'**art. 4** del Regolamento.

Da osservare che il dato personale è una definizione tecnica-giuridica per mezzo della quale il legislatore individua i diritti collegati all'identità personale. **Non è quindi il dato ad essere tutelato ma il diritto a cui lo stesso si riferisce**.

Il dato in sé è un **bene giuridico di secondo grado**.

---

15 La norma pone una **differenza** tra trattamento del dato automatizzato in tutto o in parte, sempre soggetto all'applicazione del Regolamento (anche nel caso in cui si trattasse di un solo dato di una persona fisica), e trattamento **non automatizzato** se NON contenuto in un archivio e NON destinato a figuravi rispetto a cui il regolamento **non** si applica (cfr. **C. n. 15** e 21).

16 Sulla scorta di alcune pronunzie della Corte di Giustizia UE e degli studi compiuti dal Gruppo di Lavoro ex art. 29 della Direttiva 95/46-CE (quale autorità indipendente composta da un rappresentante designato da ciascuna Autorità Garante degli Stati Membri e dal Garante Europeo della protezione dati – GEPD – ed infine dal rappresentante della Commissione Europea. Gruppo che, in base all'art. 68 del Reg. UE 679/2016, verrà sostituito dal <<***Comitato europeo per la protezione dei dati***>>).

Per dato personale si intende qualsiasi "informazione" quale il **nome**, il **codice fiscale**, l'**immagine**, un **filmato**, la **targa** di un automezzo, il numero di passaporto, **la voce**, l'**impronta digitale**, il **traffico telefonico** di una persona fisica identificata o identificabile, anche indirettamente, oppure quegli elementi riferibili ad una persona nota che può essere individuata con informazioni supplementari tanto da poterla distinguere all'interno di un gruppo o di una categoria di persone (esempio: "il cuoco stellato di Varese").

Se l'identificazione richiede l'acquisizione di ulteriori elementi per cui occorrono tempi e costi sproporzionati ed irragionevoli non sussiste identificazione e/o identificabilità. Ma bisogna ricordare che non occorre raggiungere un elevato livello di identificazione perché il dato sia assoggettato a tutela.

I dati si considerano personali se consentono l'identificazione dell'individuo oppure se le informazioni descrivono l'individuo in modo tale da consentirne l'identificazione acquisendo altri dati: entrambi i tipi di dati sono tutelati allo stesso modo.

In sostanza:

1. il dato è un concetto **dinamico** ed in evoluzione;
2. non occorre una identificazione completa o fisica della persona;
3. l'**incrocio** di informazioni, anche se detenute da più titolari, rende i c.d. dati "online" (IP e cookie, etc.) personali;
4. le tendenze sociali, economiche, professionali sono dati personali;
5. esistono le categorie particolari di dati soggette a protezione speciale e rispetto alle quali il consenso dell'interessato al trattamento deve essere particolarmente forte ed esplicito.

Il dato di cui all'art. 4 è, infatti, indicato come:

- <<**qualsiasi informazione** riguardante una **persona fisica identificata** o **identificabile** («interessato»)>>, e ivi si precisa che
- <<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**>>[17] (cfr. C26, C27, C30) e ciò senza dimenticare che, in particolare,
- il 30° Considerando precisa ancora che <<le persone fisiche possono essere associate a **identificativi online** prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli **indirizzi IP**[18], a marcatori temporanei (**cookies)** o a identificativi di

17 Cfr. i considerando (-C-) C26, C27, C30.
18 Gli **indirizzi IP** sono stati qualificati dalla Corte di Giustizia UE come **dati**

altro tipo, come i **tag di identificazione** a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare **profili** delle persone fisiche **e identificarle**>>.

Nel Regolamento **viene meno** una **definizione precisa di dati sensibili** (a differenza di ciò che è dato ritrovare nel Codice della Privacy nazionale) e, difatti, sempre all'art. 4, si trovano indicate, come detto, solo delle **categorie particolari** di dati: <<**dati genetici**>>, <<**dati biomedici**>> e <<**dati relativi alla salute**>> (già noti "in passato" come, appunto, sensibili).

"Compare", invece, la definizione di <<**pseudonimizzazione**>> quale necessaria procedura di trattamento dei dati **che**, di fatto, **impedisce di attribuire** (ricondurre) **gli stessi** <<ad 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>> (cfr. C26, C28-C29).

ACCOUNTABILITY[19]

Risulta pure rafforzato il principio di <<**accountability**>> (quale concetto del c.d. <<**dare conto**>>) e di conseguente **adeguatezza delle misure** organizzative e di sicurezza da adottare.

Si tratta di uno dei **concetti più importanti** che caratterizza il Regolamento ma non è nuovo poiché già trattato dal parere n. 3/2010 del Gruppo di Lavoro art. 29 che, infatti, da tempo, ha consigliato di richiedere

- al <<titolare del trattamento dei dati di **essere in grado di dimostrare di aver adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali**, anche attraverso l'elaborazione di specifici **modelli organizzativi**[20] e che debbano **dimostrare in modo positivo e proattivo** che i trattamenti dei dati effettuati sono **conformi al regolamento**>>.

---

personali: cfr. sentenza "Patrick Breyer in data 10/10/16 nella causa C-582/2014 e questo, anche se, per indirizzo IP, tecnicamente si intende **SOLO un'etichetta numerica che identifica univocamente un dispositivo detto host** collegato a una rete informatica che utilizza l'*Internet Protocol* come protocollo di rete.

19 Si rileva che, spesso, si riduce il concetto di <<*accountability*>> alla sola parola <<responsabilità>>. In realtà, in ambiti anglosassoni, esso ha un significato più complesso e composito quale, ad esempio, <<*la responsabilità, da parte degli amministratori che impiegano risorse pubbliche, di **rendicontarne** l'uso sia sul piano della **regolarità** dei conti sia su quello dell'**efficacia** della gestione*>>.

20 Parola che fa eco alla precedente normativa di cui al Dlgs 231/2001 che, dei Modelli Organizzativi, ne ha fatto la propria linea direttrice. E' assai probabile quindi che le future linee guida di costruzione dei modelli in materia di privacy siano simili a quelle già previste dal detto Dlgs 231/2001.

L'**art. 5** del Regolamento va in tal senso e, dopo l'elencazione di ciò che dovrebbe rappresentare ogni trattamento, ivi all'uopo richiamando i principi di <<**liceità**>>, <<**correttezza e trasparenza**>>, <<**minimizzazione**>>, <<**esattezza**>>, <<**limitazione della conservazione**>>, <<**integrità e riservatezza**>>, pone al proprio paragrafo 2 le basi del detto principio di **accountability** sancendo a chiare lettere che il titolare del trattamento deve essere pure in grado di **comprovare l'organizzazione** del **trattamento** stesso alla luce del rispetto degli anzidetti (non banali da applicare) principi.

Il titolare del trattamento, quindi, in base all'art. 25 del Regolamento dovrà:

1. **adottare misure tecniche ed organizzative** adeguate ed in grado di dimostrare che siano trattati solo i dati **necessari** ad ogni specifica **finalità** di trattamento;
2. **poter dimostrare di aver in tal modo rispettato in concreto i** non banali **principi** predetti.

Questo doppio incombente non è affatto semplice e, oltretutto, l'art. 32, parag. 1 del Regolamento alza l'asticella nel prevedere in sostanza che, "tenendo conto dello **stato dell'arte** e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone, il **titolare e il responsabile del trattamento** mettono in atto **misure tecniche e organizzative** adeguate al rischio, che comprendono, tra le altre, "**se del caso**[21]":

(a) la **pseudonimizzazione e** la **cifratura** dei dati personali;

(b) la capacità di assicurare su base **permanente la riservatezza**, l'**integrità**, la disponibilità e la **resilienza** dei sistemi e dei servizi di trattamento;

(c) la **capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

(d) una **procedura per** testare, verificare e **valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Da considerare pure che <<nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo **dei rischi** presentati dal trattamento che derivano in particolare dalla **distruzione**, dalla **perdita**, dalla **modifica**, dalla **divulgazione** non autorizzata o **dall'accesso**, in modo accidentale o illegale, a dati personali trasmessi, **conservati** o comunque **trattati**>> (art. 32, parag. 2).

21 Il Legislatore UE usa la responsabilizzante espressione "***se del caso***".

Studio Legale Tamos & Partners
www.avvocatinteam.com
Viale Piceno n. 14/a, 20129, Milano – Tel. 02/70006392 Fax 02/76113344
lorenzo.tamos@avvocatinteam.com – tel. mobile 339-6438001

TRASPARENZA - INFORMAZIONE

Anche i rafforzati obblighi di **trasparenza** ed **informazione** di cui, in particolare, agli artt. 12 e 13 del Regolamento, sono stati sottoposti al detto **restyling**.

Tutte le informazioni al soggetto interessato in sostanza devono:

1. essere date con un **linguaggio semplice** e **chiaro** (specie se si tratta di un minore: cfr. art. 8 del Regolamento);
2. avere in linea di principio la **forma scritta**, poiché l'informativa orale deve essere limitata solo se esplicitamente richiesta dall'interessato ed esclusivamente qualora l'identità di questi possa essere comprovata con altri mezzi idonei;
3. essere fornite dal titolare con **l'indicazione del periodo di conservazione** dei dati personali e del diritto dell'interessato di proporre reclamo alla autorità di controllo;
4. essere fornite **senza ritardo** rispetto a quelle che l'interessato richiede e, comunque, essere date **entro un mese** dalla richiesta quale termine **prorogabile di due** mesi, se necessario, tenuto conto della complessità e del numero di richieste;
5. essere fornite possibilmente con **mezzi elettronici** (mail) se la richiesta è pervenuta con i medesimi mezzi (salvo diversa indicazione dell'interessato).

Solo mediante una informativa chiara e trasparente si può, infatti e ad esempio, **ottenere il consenso consapevole** ed utile dell'interessato.

Il consenso in generale deve essere: 1) **inequivocabile**; 2) **libero**; 3) **specifico**; 4) **informato**; 5) **verificabile**; 6) **revocabile**; 7) a **scadenza**.

(1) **inequivocabile**: può essere implicito (mai tacito) sebbene non debba esserci dubbio che (anche col proprio comportamento) l'interessato abbia voluto dare il consenso. L'inerzia non è mai manifestazione di consenso come, ad esempio, le caselle già pre-spuntate. Deve sempre esserci una evidente azione positiva dell'utente (come quella di inserire la propria mail in un campo dove è indicata bene la finalità per la quale sarà poi usata). Il consenso deve essere sempre esplicito (art. 9) per i dati particolari o nel caso di processi decisionali automatizzati (ad es. per il caso di profilazione).

(2) **libero**: la scelta deve essere libera, non frutto di intimidazioni o raggiri, né condizionata da indicate conseguenze negative a seguito del mancato rilascio del consenso. L'articolo 7 del Reg. afferma difatti che <<nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto>>.

Non può definirsi libero il consenso dell'interessato che debba accettare di

ricevere pubblicità, o fornire dati non utili, quale condizione per conseguire la prestazione richiesta (cfr. provvedimento del Garante del 31/01/2008)[22].

(3) **specifico**: ossia inerente la finalità per la quale esiste il trattamento. Qualora il trattamento abbia più scopi il consenso dovrebbe essere prestato per ogni finalità (Considerando 32). La specificità è collegata al concetto di pertinenza con il consenso acquisito e, perciò se tale pertinenza muta, occorrerà richiedere un nuovo consenso.

4) **informato in senso sostanziale**: l'interessato deve poter conoscere i dati trattati, le modalità, le finalità ed i diritti che gli sono attribuiti dalla legge. L'interessato deve sapere, ad esempio, che in assenza di consenso non potrà accedere a determinati servizi o prestazioni o sezioni di un sito web. L'informazione si ha attraverso l'apposita informativa. Il regolamento europeo sottolinea la validità sostanziale del consenso e mette in ombra quella formale. Da ciò dipende la richiesta di un linguaggio semplice, comprensibile, persino "colloquiale".

(5) **verificabile**: non nel senso di documentale (non è infatti richiesta la forma scritta nemmeno per i dati particolari anche se in tali casi è bene usarla perché consente più facilmente di provare il consenso), ma che bisogna essere in grado di dimostrare che l'interessato lo ha dato rispetto ad uno specifico trattamento (NB: bisogna distinguere tra i vari possibili trattamenti).

(6) **revocabile**: in qualsiasi momento e la revoca deve essere semplice (tanto quanto l'atto del dare il consenso) senza che sussista alcun obbligo di motivarla. A revoca data il trattamento deve cessare (la revoca non determina illiceità del trattamento precedente ma solo l'obbligo di cessazione dello stesso), tranne nel caso in cui sussista una differente base giuridica per continuare il trattamento.

Per la revoca il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso. Nel caso in cui il titolare non ottemperi alla richiesta di cessazione, ci si può rivolgere al Garante o al tribunale per la tutela dei propri diritti.

Con la revoca si attiva il diritto alla cancellazione dei dati e, pertanto, l'azienda deve cancellare i dati del richiedente ad eccezione di quelli basati su motivi legittimi quali quelli di conservare alcuni dati per, ad esempio, mantenere un registro delle transazioni soggette ad obblighi fiscali/impositivi.

(7) **a scadenza**: perché, ovviamente, il consenso non è a tempo illimitato. All'atto della raccolta bisogna informare l'interessato sui tempi di conservazione dei suoi dati. Una volta spirati i termini di cui alla detta

22 Se, come sempre più spesso capita, il datore di lavoro pubblica la foto dei dipendenti sul sito web aziendale il consenso potrebbe ritenersi non valido perché non effettivamente libero considerato lo squilibrio di potere tra datore e suoi dipendenti. Il dipendente, infatti, potrebbe dare un consenso valido solo in circostanze eccezionali. In questi casi il consenso potrebbe non bastare per costituire la base giuridica del trattamento della fotografia.

tempistica comunicata il dato va cancellato, oppure reso anonimo. Ecco spiegato il motivo per cui in certi casi sembra preferibile una base giuridica alternativa (o aggiuntiva) al mero consenso (come ad esempio i ben ponderati "legittimi interessi" del titolare del trattamento)[23].

"PRIVACY" BY DESIGN E PRIVACY BY DEFAULT

E sempre di **restyling** (o meglio di uso di "concetti nord americani") si tratta relativamente ai principi denominati <<**Privacy by design**>>[24] e <<**Privacy by default**>> e di cui, però, la normativa europea non parla esplicitamente.

Ma il citato **art. 25** del Regolamento[25] impone concetti analoghi a quelli made in USA, ovverosia:

1. la **protezione dei dati fin dalla progettazione** (by design), e
2. la **protezione dei dati per impostazione predefinita** (by default).

In base al parag. 1 dell'art. 25 il titolare del trattamento è obbligato a compiere, sin dalla fase della **progettazione**, la **selezione di strumenti e dispositivi** necessari alla propria attività, valutando preliminarmente i tipi di

23 Attenzione: A) il consenso esplicito è l'unica base giuridica utile per il trattamento dei dati ex "sensibili". B) Per i minori il consenso è valido a partire dai 16 anni di età, prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. C) Se il trattamento dei dati è basato sul consenso dell'interessato, questi acquisisce l'ulteriore diritto alla portabilità dei dati.

24 Sono concetti usati negli Stati Uniti ed in Canada dalla fine degli anni novanta. Il riconoscimento della "*privacy by design*", quale componente essenziale nella tutela del trattamento dei dati, è stata poi conclamata alla 32° Conferenza Internazionale dei garanti della Privacy tenutasi a Gerusalemme nell'ottobre del 2010.

25 <<**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>>.

trattamento dati che porrà in essere, allo **scopo di poter pianificare** e, quindi, adottare, le più opportune misure e strumenti (by design) che permettano di rispettare in concreto il Regolamento.

In base al **parag. 2 dell'art. 25**, che introduce il concetto della protezione dei dati per **impostazione predefinita** (by default), il titolare del trattamento dovrà altresì adottare le **necessarie misure atte a garantire** che siano trattati **soltanto quei dati attinenti e necessari a ciascuna specifica finalità di trattamento** e che, quindi ed oltretutto, in forza del principi di minimizzazione dei dati trattati, siano resi a priori **inaccessibili** ad un numero indefinito di persone (senza la persona fisica).

Quindi, in concreto, il **titolare del trattamento dovrà**, come minimo:

- pre-individuare i flussi di dati in entrata, in uscita e circolanti in azienda;
- suddividere i dati trattati in essenziali e non essenziali alla propria attività ed alle sottese finalità di trattamento;
- individuare e ripartire le categorie dei dati tra quelli essenziali e non essenziali;
- individuare le persone che in azienda devono necessariamente trattare i dati per garantire il ciclo produttivo dei beni e/o dei servizi;
- progettare il trattamento "tendenzialmente" rispetto ai soli dati essenziali;
- progettare la minimizzazione del trattamento dei dati non essenziali per giungere alla ("tendenziale") esclusione degli stessi;
- progettare ed impostare la minimizzazione del trattamento riducendo la circolazione dei dati all'interno ed all'esterno dell'azienda;
- progettare, adottare, diffondere e rendere praticabili le misure e gli strumenti tecnici ed organizzativi in grado di rispettare e rendere comprovabile il concreto rispetto della normativa.

I REGISTRI DELLE ATTIVITA' DI TRATTAMENTO

L'**art. 30** del Regolamento introduce un obbligo "nuovo": la tenuta dei **registri delle attività** di trattamento.

Da precisare, in primo luogo che, in base al punto 5 dell'art. 30 del Regolamento, "**NON" sussiste l'obbligo della tenuta dei registri** per <<le 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 (i c.d. ex "dati sensibili"[26]), o i dati personali relativi a condanne penali e a

26 Difficile immaginare una società con anche un solo dipendente che non abbia in

reati di cui all'art. 10>>.

Ebbene se il dato numerico dei 250 dipendenti aiuta molto a capire l'obbligatorietà delle tenuta (con 250 dipendenti o più, difatti, i registri sono d'obbligo), l'introdotta ipotesi di **rischi** del trattamento e di un **trattamento non occasionale**, **o** che includa dati "**particolari**" di sorta, porta a suggerire (anzi a **scrupolosamente ritenere**) la necessità quasi (a priori data per) scontata della presenza dei registri in pressoché tutte le realtà aziendali un minimo organizzate.

Sia il **titolare** che il **responsabile** (e ove applicabile i loro rappresentanti) del trattamento devono, dunque, **tenere un registro scritto** (anche in formato elettronico) che, in buona sostanza, dia contezza **di chi** deve attuare **cosa**, **come**, per **quali finalità, per quanto tempo** e sulla base di quali misure di sicurezza ed organizzazione, rispetto al trattamento dei dati personali delle persone fisiche.

L'eloquenza dell'art. 30 del regolamento circa il contenuto (minimo) dei detti registri è tale che allo stesso vale la pena semplicemente rimandare[27].

trattamento dati PARTICOLARI ("sensibili").

27 - **Articolo 30 - Registri delle attività di trattamento**:

(1) Ogni **titolare del trattamento** e, ove applicabile, **il suo rappresentante** tengono un registro **delle attività di trattamento** svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni: (a) il **nome** e i **dati di contatto** del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati; (b) le **finalità** del trattamento; (c) una **descrizione delle categorie** di **interessati** e delle **categorie di dati** personali; (d) le **categorie di destinatari** a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali; (e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 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, paragr. 1.

(2) Ogni **responsabile del trattamento** e, ove applicabile, il suo rappresentante tengono un registro di tutte **le categorie di attività relative al trattamento** svolte per conto di un titolare del trattamento, contenente: (a) il **nome e i dati di contatto** del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati; (b)le **categorie dei trattamenti** effettuati per conto di ogni titolare del trattamento; (c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una **descrizione generale delle misure di sicurezza** tecniche e organizzative di cui all'articolo 32, parag. 1.

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Lo **scopo di tali registri** è quello indicato dal **considerando n. 82** del regolamento: <<**dimostrare che** [ci] **si conforma al presente regolamento**, [e che quindi] il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle **attività** di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a **cooperare con l'autorità di controllo** e a mettere, su richiesta, **detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti**>>.

Da tale quadro emerge la chiara volontà del Legislatore Europeo di obbligare il più diffusamente possibile alla tenuta di una sorta di sintetico "**ricettario**" da utilizzare come base per permettere di verificare più agevolmente se, effettivamente, quanto indicato nello stesso documento corrisponda, o meno, alla **"**realtà organizzativa privacy**"** di chi lo ha formato e lo detiene.

Dotarsi di buoni registri di trattamento, corrispondenti ad una organizzazione scrupolosa, effettiva e soprattutto adempiente alla normativa europea, **è uno dei passi da compiere per evitare istruttorie ed eventuali sanzioni**. Del resto, il fatto stesso di non poter esibire i registri, o di non averli compiutamente concepiti e tenuti, "vincolerà" in molti casi le autorità di controllo ad aprire una (più o meno severa) istruttoria d'indagine.

Da osservare che il Gruppo di lavoro ex art. 29 ha espresso il proprio **parere sul registro dei trattamenti** ove si precisa che è sufficiente che vi sia **anche una sola delle condizioni previste dall'articolo 30 per far scattare l'obbligo di tenuta del registro**[28]. Acciocché qualsiasi azienda che tratti in modo stabile dati particolari dei propri dipendenti (un'aspettativa per motivi di salute, ad esempio) dovrà dotarsi dei registri.

E oltretutto si tratta di un parere apparentemente difforme dall'interpretazione data dall'Autorità di controllo italiana che, difatti, nel proprio sito, ha precisato che, laddove si abbiano meno di 250 dipendenti e non si effettuino trattamenti a rischio (art. 30 parag. 5) la tenuta dei registri non sarebbe necessaria (e va sottolineato che l'interpretazione data dal Gruppo ex art. 29, molto più severa, è posteriore a quella data dal Garante Italiano).

DATA BREACH NOTIFICATION

Altra semi novità è data dall'**art. 33** del Regolamento spesso commentato sotto il mutuato nome a matrice anglosassone "**Data Breach Notification**".

Si tratta della **prescrizione** imposta al titolare del trattamento **di**

28 Il parere del gruppo art, 29 chiarisce anche che sarebbe bastevole registrare i soli trattamenti che attivano l'obbligo di tenuta ed, oltretutto, invita le Autorità nazionali a pubblicare un modello di registro semplificato per le piccole e medie imprese.

notificare la **violazione** degli adempimenti prescritti dal regolamento all'Autorità Garante per la protezione dei dati personali.

Tale obbligo di "**auto-denunzia**" all'Autorità deve avvenire **senza ritardo** e, ove possibile, entro **72 ore** dal momento in cui il titolare è venuto a conoscenza del sinistro, tranne nel caso in cui sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche (valutazione da compiersi in auto-responsabilità: ossia a proprio "rischio e pericolo").

Ma non basta perché la **notifica al Garante** deve anche fornire la descrizione della **natura della violazione** e, se possibile, il **numero degli interessati** dal sinistro, le probabili **conseguenze** della violazione, la descrizione delle **misure adottate** o da adottare per porre rimedio alla violazione e, sempre se possibile, **per ridurne** gli eventuali effetti negativi.

In aggiunta ciò, l'**art. 34** del Regolamento, sempre per il caso di sinistro, prevede l'obbligo di darne comunicazione senza ritardo **direttamente** alla stesso **interessato quando** la riscontrata violazione sia suscettibile di presentare un "**rischio elevato**" per i diritti e le libertà delle persone fisiche.

Detta **comunicazione diretta all'interessato non è però richiesta se**:

(a) il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione e queste erano state applicate ai dati oggetto del sinistro (misure quali la cifratura);

(b) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

(c) la comunicazione singola richiede sforzi sproporzionati e, in tal caso, si procede a comunicazione pubblica o analogamente efficace[29].

Anche da ciò emerge come, di fatto, sia indispensabile organizzare l'azienda al meglio, **progettando in modo adeguato** e **professionale** il possibile evento negativo, sia rispetto ad un eventuale **virus** che renda inservibili dei dati conservati su un computer o sul server, che avuto riguardo ad un accidentale **allagamento** che distrugga parte di un archivio cartaceo.

E' del resto ovvio che l'**assenza di progettualità della privacy aziendale** impedirà di compiere ogni e qualunque **autoanalisi seria** e credibile circa le conseguenze rischiose (elevate o meno) discendenti da un possibile sinistro: assenza che, perciò, nemmeno consentirà di valutare se davvero si avrà l'obbligo di **notificare l'evento** al diretto interessato dando così luogo ad una ulteriore serie di violazioni a pericolosa "**spirale senza fine**".

---

29 Art. 34 punto 4): <<*Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali,* ***l'autorità di controllo può richiedere****, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta*>>.

LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

Anche per i motivi appena esposti il Regolamento (**art. 35**) prevede in determinati casi una vera e propria **valutazione di impatto sulla protezione dei dati**: la c.d. **DPIA** di cui all'acronimo <<**D**ata **P**rivacy **I**mpact **A**ssessment>>.

La DPIA è prevista quando un trattamento, in particolare se basato sulle **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. In tale caso il titolare del trattamento effettua, **prima di procedere al trattamento**, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Il titolare del trattamento nello svolgere la DPIA si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

La DPIA **è richiesta, in particolare, quando**:

(a) vi sia una valutazione **sistematica** e **globale** di aspetti personali relativi a persone fisiche, basata su un trattamento **automatizzato**, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

(b) vi sia un trattamento, su **larga scala**, di categorie **particolari** di dati personali ("sensibili") o di dati relativi a condanne penali o a reati (artt. 9 e 10);

(c) vi sia la **sorveglianza sistematica su larga scala** di una zona accessibile al pubblico.

La DPIA contiene almeno:

(a) una **descrizione** sistematica dei trattamenti previsti e delle **finalità** del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

(b) una **valutazione** di **necessità** e proporzionalità dei trattamenti rispetto alle finalità;

(c) una **valutazione dei rischi** per i diritti e libertà degli interessati;

(d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Ad oggi, per capire al meglio quando si debba compiere una DPIA, bisogna guardare alle Linee Guida del 04/10/2017 adottate dal Gruppo di lavoro ex art. 29 poiché riguardanti i criteri per stabilire quando un trattamento

presenti un rischio elevato ai sensi della normativa comunitaria e, quindi, obblighi all'incombente di valutazione.

I **CRITERI** individuati sono nove e riguardano i seguenti trattamenti:

1. **valutativi** o di c.d. **scoring**, nonché di **profilazione** (ossia relativi ad aspetti concernenti il rendimento professionale, la situazione economica, la salute, gli interessi personali, le **preferenze**, **l'ubicazione** o gli **spostamenti dell'interessato**);
2. **decisioni automatizzate** che producano significativi effetti giuridici o di analoga natura (i trattamenti che determinano l'esclusione da alcuni benefici);
3. **monitoraggio** sistematico compresa la raccolta dati attraverso la sorveglianza di un'area accessibile al pubblico;
4. sugli **ex "**dati **sensibili"** (particolari) o di "natura estremamente personale" (etnia, salute, opinioni politiche, religiose, condanne penali, dati clinici);
5. trattamenti di dati su **larga scala**[30];
6. **raffronto o combinazione** di insieme di dati (il raffronto di/tra più trattamenti basati su finalità diverse ed indipendentemente dalle ragioni e/o aspettative di trattamento dell'interessato);
7. trattamenti su dati di **soggetti deboli** (anziani; degenti; minori; richiedenti asilo);
8. trattamenti innovativi e/o **scientificamente avanzati**[31] (accessi fisici mediante il riconoscimento del volto da telecamera, impronte facciali o di altro tipo);
9. trattamenti che **impediscono l'accesso ad un servizio** o di un contratto (ad esempio, lo screening di una banca, effettuato per mezzo di dati di una centrale rischi, per stabilire il diritto ad accedere ad un servizio finanziario).

Da ricordare infine che, ex art. 36 del Reg., qualora lo svolgimento della **DPIA** indichi che il trattamento potrebbe presentare un <<**rischio elevato**>>, in assenza di misure adottate per attenuare il rischio, il titolare del trattamento, **prima di procedere al trattamento stesso**, è tenuto a **consultare** il Garante della Privacy[32].

30 Il Gruppo di Lavoro ex art. 29 suggerisce di considerare su "**larga scala**" quei trattamenti con un alto numero di soggetti in assoluto o in proporzione al trattamento in questione rispetto alla popolazione di riferimento (da valutare in %), del volume dei dati e/o nell'ambito delle diverse tipologie dei dati, della durata e persistenza del trattamento, nonché dell'ambito geografico dell'attività di trattamento. Si tratta, quindi, di compiere una **autovalutazione** "guidata" solo da alcune direttive valutative astratte e a carattere generale.

31 Ed anche in questo caso si tratta di un concetto dinamico.

32 Tra l'altro la Legge di **Bilancio italiana 2018** ha "discutibilmente" modificato il

Anche in quest'ultimo caso, in disparte la legge di Bilancio 2018 che ci ha messo del suo per complicare il quadro d'insieme (cfr. la nota n. 20), sovviene l'applicazione del principio di "**autovalutazione**" e di **responsabilizzazione**. Sarà infatti il titolare del trattamento a dover, sempre a proprio "rischio e pericolo", valutare la necessità di consultare preventivamente il Garante.

DIRITTO ALL'OBLIO E ALLA PORTABILITA' DEI DATI

Si deve parlare di una sorta di parziale "**maquillage**" pure rispetto al **Diritto all'oblio** ed in parte anche per la **Portabilità dei dati** quali concetti/diritti rimarcati dal Regolamento per come disciplinati, rispettivamente, dagli **artt. 17** e **20** dello stesso.

Il **diritto alla cancellazione**, ovvero **ad essere dimenticati** (oblio), ha una propria storia trentennale (anche nazionale). In molti casi noti[33] e meno noti è difatti risultata evidente la necessità di proteggere la personalità dell'individuo attraverso il diritto ad essere (sempre più) dimenticati in relazione al **trascorrere del tempo**, tranne in alcune eccezioni.

L'art. 17 del Regolamento è in proposito apparentemente chiaro.

L'interessato ha il **diritto di ottenere dal titolare del trattamento la cancellazione** dei dati personali che lo riguardano, senza ingiustificato ritardo e il titolare ha l'obbligo di cancellarli senza ingiustificato ritardo, **se sussiste uno dei seguenti motivi**:

(a) i dati **non sono più necessari** rispetto alle **finalità** di raccolta o trattamento;

(b) l'interessato **revoca il consenso** al trattamento[34] e non sussiste altro fondamento giuridico per il trattamento;

Codice della Privacy (Dlgs 196/2003) per mezzo dei commi 1020-1025 dell'art. 1 della stessa. Nello specifico il legislatore italiano ha disposto che <<*il titolare di dati personali* [qualifica errata ed inesistente!] ***ove effettui un trattamento fondato sull'interesse legittimo che prevede l'uso di nuove tecnologie o di strumenti automatizzati***, *deve* ***darne tempestiva comunicazione al Garante per la protezione dei dati personali***. *A tal fine,* ***prima di procedere al trattamento****, il titolare dei dati invia al Garante* ***un'informativa*** *relativa all'oggetto, alle finalità e al contesto del trattamento, utilizzando il modello di cui al comma 1021, lettera c).* ***Trascorsi quindici giorni lavorativi dall'invio dell'informativa, in assenza di risposta da parte del Garante, il titolare può procedere al trattamento*** *(art. 1, comma 1022).*

33 Si ricorda il caso romano del giornale "**Il messaggero**" che, negli anni novanta, promosse un gioco a premi consistente nella ri-pubblicazione di proprie risalenti pagine in una delle quali, un bel giorno, sono ri-apparse le foto ed il nome di una persona coinvolta ("reo confesso") in un omicidio di trentanni prima. L'evidenza della inutilità sociale della "notizia" ha, quindi, comportato la condanna dell'editore e del direttore del giornale.

34 Conformemente all'articolo 6, par. 1, lettera a), o all'articolo 9, par. 2, lettera a).

(c) l'interessato **si oppone al trattamento** (art. 21) e non c'è motivo legittimo prevalente per procedere, oppure si oppone al trattamento per finalità di marketing e profilazione;

(d) i dati sono stati **trattati illecitamente**[35];

(e) i dati devono essere **cancellati per adempiere un obbligo legale** previsto dal diritto dell'Unione o dello Stato cui è soggetto il titolare del trattamento;

(f) i dati sono stati raccolti relativamente all'offerta di **servizi** della società dell'informazione rispetto ai **minori** (art. 8).

Il titolare del trattamento, **se ha reso pubblici dati personali** ed è obbligato cancellarli per i suddetti motivi, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta le misure ragionevoli, anche tecniche, per informare **gli altri titolari del trattamento**[36] che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Ma **tale cancellazione non avviene se il trattamento è necessario**:

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

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

(c) per motivi di **interesse pubblico** nella sanità pubblica (in conformità all'art. 9, par. 2, lettere h) e i), e dell'art, 9, par. 3);

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

35 Si tratta di una disposizione semplice rispetto alla quale va, però, sottolineato che essendo i dati personali connessi ad un diritto di protezione fondamentale dell'individuo, qualsiasi violazione alle disposizioni del regolamento potrebbe comportare un trattamento "illecito" e, quindi, legittimare la richiesta di revoca dell'interessato oltre che di un "sostanzioso" risarcimento danni (art. 82 reg.).

36 Qui, forse, il legislatore europeo, avrebbe fatto bene ad essere più esplicito e spiegare chi dovrebbe fare esattamente cosa e come. In assenza di una evidente contitolarità di trattamento (ex art. 26: l'esempio potrebbe essere tra una società che si occupa di collocamento ed i gestori del sito dove vengono inserite le prime domande di lavoro) l'obbligo posto a capo di un titolare di informare altri titolari rischia di ingenerare confusione e di rendere la norma in concreto inapplicata o, addirittura, inapplicabile in astratto.

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

o0o

Quanto invece al nuovo **Diritto alla Portabilità**, se non altro per meglio capirlo, bisogna tornare al concetto della (presa d'atto) della necessità di permettere la migliore circolazione dei dati personali degli individui.

In base alle linee guida del 23/12/2016, aggiornate il 5/04/2017, per come elaborate dal Gruppo di Lavoro ex art. 29 circa tale diritto alla portabilità, lo **scopo primario** sarebbe quello di **aumentare il potere di controllo degli interessati** sui propri dati personali.

La facilitazione informatizzata della trasmissione diretta dei dati da un **ambiente informatico all'altro** consentirebbe, quindi, il raggiungimento di tale obiettivo aumentando **la necessaria concorrenza tra gli operatori** (titolari del trattamento) all'interno del mercato europeo: si tratta quindi, senza dubbio, di un ulteriore importante monito (**scopo "non secondario"** della normativa) rivolto a tutte le aziende soggette all'applicazione della normativa onde stimolarne l'organizzazione rispetto alla c.c. "questione privacy" da considerare sempre più come una sorta di "imposto" punto di forza ovvero di rafforzamento aziendale.

L'**art. 20** è chiaro. L'interessato ha diritto di ricevere in un **formato strutturato**, di uso comune e **leggibile da dispositivo** i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto **di trasmettere** tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha inizialmente forniti se:

1. il trattamento si basi **sul consenso**[37] (art. 6, par. 1, lettera a, o art. 9, par. 2, lettera a), o su un contratto (art. 6, par. 1, lettera b), **e**
2. il trattamento sia effettuato con **mezzi automatizzati**.

In tali casi l'interessato ha il diritto di ottenere la **trasmissione diretta** dei dati personali **da un titolare del trattamento all'altro**, se tecnicamente fattibile.

L'esercizio di questo diritto lascia impregiudicato il diritto alla cancellazione e non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri portati dal titolare del trattamento.

E precisa infine la norma – ad "ampia" chiusura cautelativa della stessa – che, in ogni caso, si tratta di **un diritto che non deve ledere i diritti e le libertà altrui**, poiché, in sostanza, viene pure posto un principio di responsabilizzazione dell'interessato rispetto all'esercizio del potere in tal modo concessogli.

37 Se il trattamento è stato avviato da una autorità senza il consenso dell'interessato, non potrà essere questi a richiederne la trasmissioni ad altri soggetti.

o0o

IL RESPONSABILE DELLA PROTEZIONE DEI DATI

E nemmeno è del tutto nuova la introdotta figura del **Responsabile della Protezione dei dati** (**D.P.O.**: acronimo di <<**D**ata **P**rotection **O**fficer>>) di cui all'**art. 37** del regolamento, atteso che è una sorta di evoluzione della figura del "**privacy officer**" di cui all'art. 18 della citata Direttiva 95/46/CE (figura che consentiva di avere benefici o esoneri di varia natura a favore delle imprese che di tale soggetto indipendente deputato al controllo facevano uso).

Circa una ventina di paesi dell'unione hanno variegatamente disciplinato negli anni tale figura[38] e questo benché le origini storiche siano da ricondurre al "Chief Privacy Officer" di matrice statunitense, per come sviluppatasi oltre oceano soprattutto negli anni novanta.

TRE sono i casi in cui il Titolare ed il Responsabile del trattamento debbono sempre, sistematicamente (ex art. 37), **designare un DPO**[39]:

1. se il trattamento è effettuato da una **autorità pubblica** o da un organismo pubblico, eccettuate le autorità giurisdizionali nell'esercizio delle funzioni giurisdizionali;
2. se le **attività principali**[40] 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**[41] degli interessati su **larga scala**[42];

---

38 L"Italia, con le linee guida in materia di dossier sanitario, adottate il **04/06/2015** (GU n. 146 17/07/2015) ha già messo in luce (per voce del Garante nazionale) l'auspicabile nomina di un DPO in materia sanitaria che possa occuparzi anche dei casi di c.d. "Data Bresch" (sinistri) collaborando con il Garante stesso.

39 Il DPO può anche essere comune a più soggetti, pubblici o privati. Un gruppo imprenditoriale può avere un solo DPO a condizione che questi sia facilmente raggiungibile da parte di ciascun membro del gruppo.

40 Le attività principali sono indicate dal **97° considerando** in quelle <<***primarie*** *che esulano dal trattamento dei dati personali come attività accessoria*>> e per le linee guida (punto 2.1.2.) sono <<*le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese quelle attività per le quali il trattamento dei* ***dati è inscindibilmente connesso all'attività*** *del titolare o del responsabile*>>. Il trattamento dei dati sanitaria dei degenti di **un ospedale contenute nelle cartelle cliniche** è da ritenersi attività principale posto che senza di essi la degenza e le cure non sarebbero somministrabili e, quindi, il DPO va senza dubbio nominato.

41 Sempre secondo le linee guida per **regolare** e **sistematico** si intende rispettivamente (A) "continuativo"; "intermittente ad intervalli regolari"; "costante"; (B) "che avviene per sistema"; "organizzato-metodico"; "nell'ambito d un progetto complessivo di raccolta dati"; "svolto nell'ambito di una strategia": verrebbe quindi da dire, provocatoriamente, che il DPO sarebbe SEMPRE da nominare posto che una buona progettualità ed organizzazione della privacy di una aziendale di medie dimensioni non può prescindere da ciò!

42 Per capire cosa sia la <<**larga scala**>> occorre riferirsi al **91° considerando** in

3. se le attività principali del titolare o del responsabile del trattamento consistono nel trattamento, su **larga scala**, di "**dati particolari**" (art. 9) o dati relativi a **condanne penali** e **a reati** (art. 10).

Il DPO deve avere delle **qualità professionali e la conoscenza specialistica** della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i propri compiti di controllo e collaborazione con le autorità e può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure, preferibilmente, essere un soggetto esterno ed assolvere i suoi compiti in base a un contratto di servizi.

Il titolare o il responsabile del trattamento **pubblicano i dati** di contatto del DPO e li **comunicano all'autorità di controllo**.

In base all'art. 38 il **titolare e il responsabile del trattamento**:

- si assicurano che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati;
- lo sostengono nell'esecuzione dei suoi compiti fornendogli le risorse necessarie per assolverli e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;
- si assicurano che non riceva alcuna istruzione circa l'esecuzione dei suoi compiti senza rimuoverlo o penalizzarlo per l'adempimento degli stessi;
- fanno in modo che gli interessati possano contattarlo per tutte le questioni relative al trattamento dei dati e per l'esercizio dei loro annessi diritti.

Il DPO è tenuto al **segreto** o alla **riservatezza** in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri e può svolgere altri compiti e funzioni che non diano adito a un conflitto di interessi.

I principali **compiti** – minimi – **del DPO** (art. 39) sono di:

- **informare** e **fornire consulenza** al titolare o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- **sorvegliare** l'osservanza del regolamento, di altre disposizioni

base a cui sarebbero su larga scala quei trattamenti che <<*mirano al trattamento di una notevole quantità di dati personali a* ***livello regionale***, ***nazionale*** *o* ***sovranazionale*** *e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano* ***un rischio elevato***, *ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché* ***ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati***, *specialmente qualora* ***tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti***>>.

dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo;

- **fornire**, se richiesto, un **parere** in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- **cooperare con l'autorità** di controllo e fungere da punto di contatto per la stessa per questioni connesse al trattamento, tra cui la consultazione preventiva (art. 36), ed effettuare, se del caso, consultazioni relative a qualunque altra questione;
- **considerare** bene **i rischi del** trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e finalità del medesimo.

o0o

(3) LA RESPONSABILITA' E LE SANZIONI

Le responsabilità e le sanzioni introdotte dal regolamento sono davvero serie e da non sottovalutare.

Uno degli aspetti che meriterebbe una certa attenzione tra i molti posti dalla normativa europea è dato dai 6 punti che compongono l'**art. 82** del Regolamento. L'eloquenza della disposizione è tale che nemmeno necessiterebbe di particolari commenti perché, in disparte la fastidiosa ridondanza della parola "trattamento", **il concetto** ivi **espresso appare chiaro**: i **danni da illecito** (da leggersi come "inadeguato") utilizzo dei dati dei privati **verranno risarciti dai responsabili e dai titolari** del trattamento degli stessi.

Le responsabilità

Quindi, in altre ancor più semplici parole, a pagare non sarà solo direttamente la società, ente, associazione, da intendersi quali autonomi soggetti giuridici, bensì la persona (fisica) a cui la responsabilità da cattivo trattamento dovrà essere imputata e che, peraltro, non è detto coincida (sempre e solo) con il legale rappresentante della società, ente, associazione di cui si tratti.

L'Art 82[43] prevede invero espressamente che <<**chiunque** subisca un

43 **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.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

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**>>.

Il **titolare** del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento.

Il **responsabile** del trattamento risponde invece per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti allo stesso o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Entrambi i soggetti sono **esonerati** dalla responsabilità se dimostra che l'evento dannoso non è loro in alcun modo imputabile. **E sarà ben difficile che potranno essere davvero esonerati qualora in azienda manchi e/o sia carente un adeguato apparato organizzativo in materia di Reg. 679/2016**.

Titolare e responsabile del trattamento (ovvero più titolari e più responsabili del trattamento) sono **responsabili in solido** per l'intero ammontare del danno al fine di garantire il risarcimento effettivo dell'interessato: e questo salvo il caso in cui uno di loro paghi, sussistendo la facoltà di esercitare il diritto di regresso rispetto alla quota parte di risarcimento dovuto dagli altri responsabili che non abbiano pagato.

Le sanzioni

Quanto poi alle sanzioni – pur tenendo conto delle linee guida relative alla loro applicazione adottate dal gruppo di Lavoro ex art. 29 in data 03/10/2017 – **c'è davvero poco da scherzare** vuoi perché trattasi di normativa sovranazionale direttamente applicabile, vuoi perché, nonostante l'applicazione soft che ci si attende per i primi tempi (dal 25 maggio 2018, sino alla fine del 2019?), il peso delle stesse si farebbe comunque sentire.

Anche in questo caso **l'art. 83** del Regolamento che prevede il detto apparato sanzionatorio (in termini di condizioni generali di applicazione) parla

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al par. 2.
6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'art. 79, par. 2.

da sé. Esso prevede innanzitutto che ogni autorità di controllo nazionale provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso **effettive**, proporzionate e **dissuasive**, nonché:

- inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta ad altre misure (art. 58), o in luogo di tali misure;
- tenendo conto di tutta una serie di elementi, tra cui: a) natura, gravità e durata della violazione, dell'oggetto e finalità del trattamento in questione, del numero di interessati lesi dal danno e il livello del danno da essi subito; b) carattere doloso o colposo della violazione; c) **misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno subito dagli interessati**; d) responsabilità del titolare o del responsabile del trattamento **tenendo conto delle misure organizzative da essi messe in atto**; e) precedenti violazioni pertinenti commesse dal titolare o dal responsabile del trattamento; f) cooperazione con l'autorità di controllo al fine di porre rimedio e attenuarne i possibili effetti negativi; g) categorie di dati personali interessate dalla violazione; etc.

La violazione delle disposizioni attinenti agli obblighi del titolare e del responsabile del trattamento, ovvero attinenti agli obblighi degli organismi di certificazione e agli obblighi (alias: poteri) delle autorità di controllo è soggetta a sanzioni amministrative pecuniarie **fino a 10.000.000,00 di euro**, o per le imprese, fino al **2%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

E' invece soggetta a sanzioni amministrative pecuniarie **fino a 20.000.000,00 di euro**, o per le imprese, fino al **4%** del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, la violazione delle disposizioni seguenti:

(a) i **principi di base del trattamento**, comprese le condizioni relative al consenso[44];

(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;

(d) **qualsiasi obbligo** ai sensi delle inerenti legislazioni degli Stati;

(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, parag. 1.

Ovviamente l'esercizio da parte dell'autorità di controllo dei poteri attribuitile dall'art. 83 è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

44 A norma degli articoli 5, 6, 7 e 9.

Gli Stati membri, in base all'art. 84, stabiliscono inoltre le norme relative alle altre sanzioni soprattutto per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, nonché adottano tutti i provvedimenti necessari per assicurarne l'applicazione.

A ciò si aggiunga che sono in dirittura d'arrivo le ulteriori **modalità con cui potersi rivolgere al Garante della Privacy**, al fine di segnalare un operatore economico e contestarne le modalità con cui sono trattati i dati personali da parte di questo.

Vi è lo strumento del <<**reclamo**>> che può essere trasmesso dall'interessato o, a protezione dell'interessato stesso, direttamente <<da un **ente del terzo settore** soggetto alla disciplina del decreto legislativo 3 luglio 2017 n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati>> (cfr. art. 28, schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE n. 679/2016).

Inoltre, a prescindere da un reclamo dell'interessato, <<**chiunque**>> (ossia, ogni soggetto che lo desideri, oltre all'interessato) potrà rivolgere al Garante <<una **segnalazione**>> verso un altro soggetto che detiene inadeguatamente dati personali e, quindi, in tal modo, attivare una procedura d'ufficio.

o0o

4) RIFLESSIONI CONCLUSIVE

Oggi è accresciuta la percezione che i dati personali delle persone fisiche rappresentino un valore appartenente all'individuo a cui gli stessi si riferiscono, oltre che un vero e proprio diritto meritevole di ampia tutela.

E' peraltro plausibile ritenere che, a breve, la detta mera percezione si trasformi in piena generale consapevolezza dell'esistenza di un diritto fondamentale e, quindi, i dati personali verranno considerati dalla generalità delle genti **al pari della salute** e della **proprietà privata** e ciò comporterà delle incontenibili conseguenze sui mercati.

o0o

Adeguarsi non è, quindi, solo una questione di obblighi

Stiamo infatti assistendo ad un **passaggio storico** che apre una opportunità soprattutto per chi si saprà percorrerlo, valutando **i tempi e la domanda di protezione** che, sempre più, verrà rivolta ai e sui mercati da parte dei privati (e non solo).

Ignorare o l**imitarsi ad inseguire** "all'ultimo minuto" la crescente domanda di tutela di questo valore-diritto e sempre più sentita esigenza sarà rischioso, **controproducente** e, soprattutto, molto (più) **costoso**.

Le aziende che prima delle altre adotteranno dei buoni modelli organizzativi in materia di trattamento dati non dovranno temere le future

richieste dell'utenza, le fasi ispettive dell'autorità di controllo, le sanzioni, le richieste di risarcimento da parte dei privati e, in generale, il "**nuovo mondo**" che, nel "bene e nel male", ha in tal modo aperto un ulteriore scenario che, forse, andrebbe semplicemente assecondato, visto che ignoralo non si può.

Chi crede si tratti solo dell'ennesima "seccante" normativa da c.d. "**burocrati europei**" **sbaglia di grosso**.

Si provi del resto a pensare al fatto che nel mondo digitale è stata già creata una **apposita moneta** (**bitcoin**[45]) come se si trattasse di un vero e proprio "Stato" a sé stante, parallelo a quello materiale e finanziario "classico": il "conio" della valuta monetaria è, infatti, uno dei primi passi che compie uno "Stato" per legittimare sé stesso.

Se poi si considera che la detta **moneta** digitale è basata sulla detenzione ed il trasferimento di **pacchetti di dati** indirettamente **riconducibili alle transazioni effettuate dalle persone**[46], ci si rende conto che un nuovo mondo esiste, è funzionale da tempo e, forse, **non può essere sottovalutato** o ignorato.

E questo poiché se è vero che nel nuovo ambito monetario (della **criptovaluta**) la protezione della persona fisica è paradossalmente di altissimo/pressoché impenetrabile livello, altrettanto non si può dire per tutti i servizi, prodotti e relative transazioni a cui pure la detta valuta, in quel vastissimo mercato, fa (nel bene e nel male) sempre più riferimento.

Invero, a parità di servizio o prodotto, la "protezione" del dato personale offerta all'utente rispetto ad una transazione compiuta in bitcoin non è lontanamente paragonabile alla transazione tradizionalmente offerta da un operatore medio di mercato. La prima è assoluta, il dato della persona fisica non è difatti sfruttato nell'ambito della transazione, la seconda è invece relativa in quanto espone l'utente al rischio che i propri dati personali vengano trattati bene o male.

o0o

45 Cfr. Wikipedia: <<il B-bitcoin (codice: BTC o XBT) è una **criptovaluta** e un sistema di pagamento mondiale creato nel 2009 da un inventore noto con lo pseudonimo di Satoshi Nakamoto, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008. Per convenzione se il termine Bitcoin è utilizzato con l'iniziale maiuscola si riferisce alla tecnologia e alla rete, mentre se minuscola (bitcoin) si riferisce alla valuta in sé. La rete Bitcoin consente il possesso e il **trasferimento anonimo** delle monete; i dati necessari a utilizzare i propri bitcoin possono essere salvati su uno o più *personal computer* o dispositivi elettronici quali *smartphone*, sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca. In ogni caso, i bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un "indirizzo bitcoin". La struttura peer-to-peer della rete Bitcoin e la mancanza di un ente centrale rende impossibile a qualunque autorità, governativa o meno, il blocco dei trasferimenti, il sequestro di bitcoin senza il possesso delle relative chiavi o la svalutazione dovuta all'immissione di nuova moneta>>.

46 I cui dati personali sono stati, paradossalmente, resi anonimi e pressoché indecifrabili dal sistema/mercato privato sviluppatosi in rete.

In definitiva l'emergente equazione di possibile riferimento è piuttosto semplice e si basa su cinque punti:

1. accresciuta consapevolezza generale della preziosità dei dati personali;
2. esigenza (reale e/o pure "speculativa") di protezione degli stessi;
3. affermazione di un diritto fondamentale;
4. "nuovo mercato" in cui la protezione può essere assicurata oppure no;
5. spostamento della domanda nel mercato e tra mercati.

Varrebbe forse la pena rifletterci sopra... non troppo a lungo però!