SOMMARIO

1 PRINCIPI DI PRIVACY

1.1 CENNI STORICI

Il concetto di privacy è un concetto variabile, mutevole e culturale. È variabile in quanto vi è una correlazione tra il concetto di privacy e l'evoluzione delle nuove tecnologie dell'informazione e della telecomunicazione (ICT). Il termine privacy nasce nel 1890, anno di pubblicazione di un articolo scritto da due noti giuristi americani, ovvero **Samuel Warren** e **Louis Brandeis**. Il primo era un noto avvocato di Boston, mentre il secondo un magistrato americano. L'articolo da loro pubblicato era intitolato "***The right to privacy***", ovvero il diritto alla privacy. Quando si invoca un nuovo diritto, bisogna chiedersi il perché nasce questa esigenza. Questo articolo viene infatti scritto in quanto in quel periodo si andava diffondendo la stampa, i giornali, che andavano a raccontare di fatti e di persone che vivono in quella determinata realtà. Ciò che fece saltare i nervi a Warren fu il termine con cui venne definita la moglie, ovvero "**regina dei salotti**". Warren sentì "attaccata" la propria proprietà privata, la propria famiglia e la propria intimità. Warren rivendicava quindi il **diritto di essere lasciato da solo**, diritto attaccato sia dalla stampa che dalle foto (perché proprio in quel periodo nacquero le prime macchine fotografiche). Per la prima volta si parla quindi del diritto al rispetto della vita privata di una persona, della propria intimità. Privacy non significa solo rispetto della vita privata, ma rispettare anche i sentimenti, l'aspetto più intimo di una persona, le sue emozioni. In questo caso si va a trattare la privacy dell'uomo in maniera simile al diritto della proprietà privata e del *"**let to be alone**"*.

In Italia il primo a parlare di riservatezza fu **Massimo Ferrara Santamaria**, che teorizzò un diritto analogo nel 1937, con la pubblicazione de "Il Diritto alla Illesa Intimità Privata". I primi casi di personaggi famosi italiani che furono coinvolti in controversie giudiziarie relative al diritto alla riservatezza furono:

- **Enrico Caruso**: ci furono contestazioni da parte degli eredi, riguardanti la lesione della privacy del tenore, successivamente all'uscita di due film, in particolare "Enrico Caruso, Leggenda di Una Voce" (1951), poiché trattavano fatti dell'infanzia di Caruso, per lo più fittizi;
- **Claretta Petacci**, in merito alla sua relazione con Benito Mussolini. Nel 1963 la Corte di Cassazione confermò definitivamente la condanna al settimanale «Tempo» (all'epoca uno dei principali settimanali italiani), per aver pubblicato, in un servizio sulla Petacci, diversi particolari inerenti alla sua vita intima. La sentenza applicò il principio secondo il quale non vanno rese note vicende che riguardano la sfera privata delle persone, anche di quelle famose, in assenza d'interesse pubblico.

In ambito internazionale si ricorda il caso della principessa egiziana **Soraya Esfandiary Bakhtiari** (1932-2001) in relazione ad una sua storia d'amore. L'ex regina consorte dell'ultimo scià di Persia, Mohammad Reza Pahlavi, fece causa ad alcune testate giornalistiche sostenendo che la propria riservatezza era stata violata: i giornali avevano ritratto la donna mentre era in compagnia di un uomo dentro la propria abitazione. In questo caso cui viene riconosciuto il diritto della riservatezza del cittadino, senza l'esistenza di una normativa. La giurisprudenza comincia a ragionare, capisce che la foto viene scattata in un luogo privato e che ogni persona ha diritto alla riservatezza. Il diritto alla riservatezza è un qualcosa che riguarda la propria intimità, al riparo dagli sguardi molesti. Erano però vincolati dal fatto che non esisteva l'articolo a tal riguardo. Viene quindi utilizzato **l'articolo 2 della Costituzione**, usato per garantire la riservatezza della persona, in quanto diritto inviolabile della persona, che può essere lesa solo in atto di un diritto costituzionalmente rilevante. Altro caso internazionale di rilievo fu Nel 1964, negli Stati Uniti, il sottosegretario di stato e deputato **Sullivan**, cita a giudizio il NYTimes, in quanto aveva pubblicato una serie di dati che riguardavano l'utilizzo di soldi pubblici. Lui quindi se la prende con la stampa perché pubblica cose "personali". La corte alla fine diede ragione al NYTimes, perché c'è il diritto da parte del cittadino di sapere cosa si fa con i soldi pubblici (che sono appunto concessi con finalità pubblica e non privata).

Parlando di normative, il primo documento in materia di protezione dei dati personali in Italia fu la **legge 675** che fu cambiata fino ad un totale di 13 volte. Si è decisi poi di avere un testo unico, ovvero il così detto **Codice Privacy**, entrato in vigore il primo gennaio 2004. Questo era composto da 186 articoli e 8 allegati. Era un testo

ben congeniato, tutt'ora in vigore. Dei 186 articoli però solo 27 sono ancora in vigore, mentre gli altri sono stati eliminati in quanto ripetizione degli articoli del regolamento europeo (come l'articolo 13) o in contrasto con essi. Per gli informatici è interessante **l'allegato B**, in quanto conteneva le misure minime di sicurezza, approccio che è stato completamente rivoluzionato con l'utilizzo della nuova normativa europea in materia di privacy.

1.2 LA PRIVACY CON L'AVVENTO DEL WEB

Ormai siamo in un periodo in cui ognuno di noi condivide e mantiene due persone distinte, il cosiddetto **corpo fisico** ed il **corpo elettronico**: Ultimamente, oltre al nostro corpo tangibile, abbiamo creato un certo corpo *"volatile"*, che corrisponde all'insieme di dati che ci rappresentano sul web. Spesso vengono utilizzate tecnologie (cookies di terze parti) per raccogliere informazioni su di noi e realizzare un profilo digitale delle nostre abitudini, passioni, hobby e ricerche creandoci appunto un'identità digitale che spesso può essere anche molto diversa da quella fisica ma che comunque fa parte del nostro essere e per tale dovrebbe rimanere illesa mentre spesso viene usata come merce di scambio tra aziende. Se ne parlava già nel 1973, quando S**tefano Rodotà** aveva fatto notare come gli elabori elettronici sarebbero diventati i nuovi strumenti di controllo dei cittadini ("*Elaboratori elettronici e controllo sociale*"). Ad oggi Internet è il più grande spazio pubblico attualmente esistente ma anche il più grande esperimento di socialismo informatico. Chi ha ora le info ha il potere di controllare le persone. Siamo immersi in questa realtà piena di interazione, di opportunità e di annunci "free" che spesso ci fanno dimenticare cosa diamo in cambio per tutto ciò, i nostri dati. La rete diventa uno strumento di controllo e sorveglianza su scala mondiale; questo spazio quindi, da che era uno spazio di assoluta libertà, è diventato oggi uno strumento di controllo, di sorveglianza, di repressione a cui siamo chiamati direttamente a difenderci. Tutto ciò ci avvia verso un processo di chiarificazione, un mondo di luce perenne, ovvero un mondo senza segreti. Il diritto alla **privacy** ci viene in aiuto in tutta questa visione di trasparenza e la normativa ci protegge e avvolge la nostra identità digitale andando a porre dei paletti a vari aspetti; esso corrisponde *al diritto della riservatezza, diritto alla protezione dei dati personali, all'identità personale, all'oblio, alla dignità umana, alla tutela dell'animo, al mutamento del concetto tradizionale di privacy*,*al diritto ad essere lasciato da solo, al diritto di mantenere il controllo sulla circolazione delle informazioni che riguardano l'interessato*. Tutto ciò è riportato nell' articolo 8 della Carta dei diritti fondamentali dell'U.E. Questo articolo è importante in quanto sancisce a livello europeo dei principi fondamentali importantissimi, ovvero:

1) Ogni individua ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2) I dati devono essere trattati secondo principi di **lealtà**, **finalità** e in base al **consenso** della persona interessata. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3) Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Altro elemento chiave è rappresentato dalla Dichiarazione dei diritti in Internet. Viene elaborata nel 2015 da una commissione eterogenea, presieduta da Stefano Rodotà e composta da altri giuristi, ma anche informatici, ingegneri informatici, matematici, sociologi ed economisti. Al suo interno vengono riconosciuti quelli che sono i diritti fondamentali del cittadino di Internet; è quindi una vera e propria carta dei diritti della rete.

2 GDPR

Dal 25 maggio 2018 è direttamente applicabile in tutti gli stati membri il Regolamento generale sulla protezione dei dati – UE 2016/679, meglio noto come **General Data Protection Regulation** (GDPR) composto da 99 articoli e 173 considerando. L'oggetto del regolamento europeo è quello di garantire la libera circolazione dei dati nell'assoluto rispetto dei diritti fondamentali della persona. Il suddetto regolamento

sancisce le modalità per la protezione dei dati personali delle persone fisiche e la condivisione delle relative informazioni. Prevede, dunque, adempimenti per aziende e professionisti (alcuni dei quali già presenti nel **Codice privacy**) e sanzioni per i titolari di dati altrui in caso di mancata protezione degli stessi (al riguardo e a titolo esemplificativo si menziona il Data Breach, l'esposizione non autorizzata delle informazioni). Il regolamento europeo in materia di protezione dei dati personali è lo strumento normativo di cui bisogna tenere conto quando abbiamo problemi di protezione della privacy. Il regolamento europeo è una fonte del diritto europeo e ha il fine di uniformare la tutela della protezione dei dati personali in modo omogeneo in tutti i paesi dell'unione europea, tale regolamento nasce proprio dall'esigenza di aggiornare la normativa in materia di protezione dei dati personali per far fronte ai nuovi abusi e gestioni che vengono imposte sui dati soprattutto sul web. Il regolamento europeo è direttamente applicabile, quindi non ha bisogno di una legge dello stato che lo recepisca e deve essere applicato ad ogni persona all'interno dell'unione europea, quindi anche le multinazionali quali *Google*, *Apple*, *Amazon* che non hanno la loro sede legale in Europa hanno l'obbligo di trattare i dati dei propri utenti europei secondo il GDPR. La normativa nasce dall'esigenza di standardizzare i trattamenti all'interno dell'UE e dal dovere di **responsabilizzare** (tramite il principio accountability) le persone che trattano questi dati (titolare del trattamento). Il parlamento europeo quindi per evitare di avere una frastagliata normativa che cambiava di paese in paese, ha deciso di provvedere con il regolamento. Questo regolamento è quindi uguale in tutti i paesi dell'UE. In Italia si è deciso di adeguare il vecchio decreto al regolamento GDPR. Quindi abbiamo una fonte europea (GDPR) e il decreto legislativo adeguato al regolamento che già forniva una buona comprensione in ambito di privacy e che con l'avvento del GDPR è stato ulteriormente corretto e ampliato. In particolare dall'articolo 4 ricaviamo la definizione che il GDPR dà al concetto di **dato personale**:

> 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)

2.1 TRATTAMENTO DEI DATI

La normativa, nell'articolo 4, fornisce varie definizioni atte a far comprendere al meglio i concetti che si possono trovare al suo interno. Per evitare quindi un indiscriminato processo di trattamento dei dati, sono stati posti dei paletti, in quanto si è definito cosa si intende per **trattamento dei dati:**

> 2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

I principi fondamentali al trattamento dei dati sono contenuti nell'articolo 5 che è il cuore del regolamento. Tra questi principi ovviamente troviamo **l'equità**, la **trasparenza**, la **minimizzazione** del dato (principio di necessità, utilizzo solo i dati necessari per una determinata finalità), **esattezza** ed **aggiornamento** del dato, **limitazione nella conservazione** del dato (per quanto tempo devo conservare il dato), principio di **integrità** e **riservatezza** (i documenti devono essere immodificabili), sicurezza e **notificazione della violazione**, **privacy by design** (alcune misure devono essere progettate dalla fase del concepimento) e **privacy by default** (regole fissate già da provvedimenti normativi). Con privacy by design ci si riferisce alla necessità di prevedere già in fase di progettazione dei sistemi informatici e applicativi, sistemi che tengano sotto controllo i rischi che il trattamento può comportare per la tutela degli interessati. Privacy by default si ha tutte le volte in cui un soggetto cede i propri dati ad un terzo e, quindi, v'è una procedura interna che preveda e disciplini le modalità

di acquisizione, trattamento, protezione e modalità di diffusione. I 3 elementi fondamentali sui quali si fonda il regolamento europeo sono **accountability**, **trasparenza dei dati** e **affidabilità.** Il codice rispetto alla vecchia disciplina accoglie quelli che sono i principi generali e introduce strumenti per concretizzare questi principi. I principi generali sono quelli di minimizzazione, essenzialità del dato, pertinenza ecc. e cerca di renderli più concreti con dei nuovi strumenti che dovrebbero aiutare il titolare del trattamento.

All'interno del GDPR ci sono catalogati e previsti diverse tipologie di dato, tale diversità nasce dalla natura di questi dati che può essere diversa e che può, nel caso di illeciti, portare a conseguenze più o meno gravi per l'interessato. Proprio per questo la normativa prevede una definizione accurata dei dati e su come tali dati devono essere trattati in base alla loro tipologia. Le diverse tipologie di dati sono:

- Personale
- Identificativo
- Particolare (Sensibile)
- Giudiziario
- Biometrico
- Genetico
- Relativo allo stato di salute
- Relativo all'ubicazione
- Anonimo

Sui dati sensibili interviene l'articolo 9 che regolarizza affermando che "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Come già scritto in precedenza, tale normativa non impone un fermo sul trattamento e sulla condivisione dei dati ma va a regolarizzare i processi. Questo articolo infatti prevede, al seconda comma, diverse eccezioni necessarie: *Il trattamento dei dati è possibile se consentito, se vi è un rapporto di lavoro, per difendere un diritto in sede giudiziaria, ai fini medici o per salvare la vita all'interessato*.

2.2 DIRITTI DELL'INTERESSATO

Una delle differenze sostanziali tra il vecchio codice privacy e il GDPR è la sezione in cui vengono definiti in maniera esaustiva i diritti dell'interessato. Tali diritti previsti con la nuova normativa sono riassunti in:

Il rispetto dei diritti dell'interessato (CAPO III ARTT. 15, 16, 17, 18, 20, 21)
Il Regolamento formalizza un ampio catalogo di diritti che spettano all'interessato. Si tratta del diritto di accesso, del diritto di rettifica, del diritto alla cancellazione (più noto come diritto all'oblio), diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione al trattamento, con gli eventuali connessi obblighi di notifica/comunicazione gravanti sul titolare.

Il particolare caso dei processi decisionali automatizzati (CAPO III – art. 22)
E' riconosciuto il diritto dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona. Tra le operazioni contemplate dalla norma troviamo la profilazione (così come definita dall'art. 4.1, n. 4). Il relativo divieto non si applica ove la decisione si basi sul consenso esplicito dell'interessato, sia necessaria per l'esecuzione di un contratto con l'interessato, ovvero sia autorizzata dal diritto dell'Unione o del singolo Stato membro.

2.3 TITOLARE DEL TRATTAMENTO

Dall'articolo 4 troviamo la definizione fornita dal GDPR: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento*

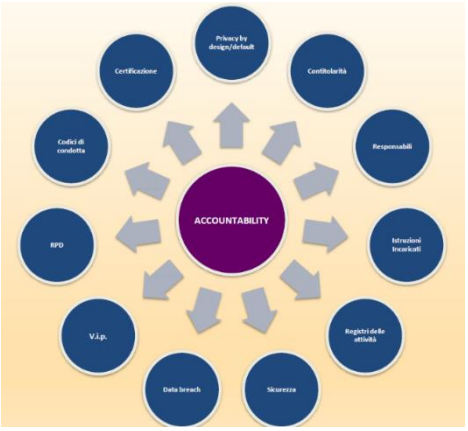
di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74) .

Questo significa che il titolare del trattamento deve rendere conto che nel trattamento dei dati che opera, rispetta la normativa. Quindi se dovesse esserci un illecito, il responsabile è il titolare del trattamento, salvo problemi a lui non imputabili. Articolo 32 dice 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 fisiche, il **titolare del trattamento** e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un **livello di sicurezza adeguato al rischio**. Il titolare del trattamento, essendo che è colui che meglio conosce l'assetto organizzativo è proprio quella persona che attraverso, un'opera di **autoanalisi,** deve riuscire a porre in essere le misure necessarie atte a gestire i rischi riguardanti i dati. Al titolare di trattamento viene lasciata quindi anche la libertà di rilevare le misure di sicurezza più adeguate rispetto al contesto nel quale opera e rispetto al tipo di dato che tratta. Il titolare deve quindi avere un comportamento proattivo. Tutto quello che stiamo vedendo serve a fornire al titolare del trattamento i principi e gli strumenti per rendere legittimo il trattamento dei dati ed il regolamento fornisce proprio tali strumenti. Anzitutto abbiamo la nuova figura del **responsabile dei dati personali**, che non si sostituisce al titolare del trattamento, ma è una figura di supporto, in quanto gli fornisce pareri, attua determinate misure, fa da interfaccia, per esempio in ambito universitario, tra studenti dipendenti ed università, ma non si sostituisce al titolare. Il regolamento oltre a stabilire i ruoli, indica come i dati devono essere trattati, e inoltre ci dice quali sono i requisiti che devono avere i dati.

2.4 ACCOUNTABILITY

Il principio di accountability è la novità apportata dalla nuova normativa che va a responsabilizzare il **titolare del trattamento**. Tale principio significa che il titolare deve porre tutte le misure atte a mitigare i rischi sui dati, ed inoltre deve dare prova di aver fatto questo, lasciando quindi traccia di tutte le operazioni finalizzate a tutelare i dati. **L'articolo 24** prevede appunto il principio di accountability:

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.



Grossa differenza con il vecchio codice privacy è che prima si imponevano delle misure di sicurezza minime, mentre ora il regolamento attuale non dice nulla, dice solo che vanno adottate le misure di sicurezza che si ritengono opportune. La **gestione del rischio** grava dunque sul titolare del trattamento e ciò valorizza il concetto di accountability e di responsabilizzazione del titolare del trattamento.

La politica utilizzata nel GDPR, rispetto al vecchio codice Privacy, è l'adozione di comportamenti **proattivi** e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

La protezione dei dati deve passare *"dalla teoria alla pratica"*. Gli obblighi giuridici devono essere tradotti in misure concrete di protezione dei dati e in questo caso l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente. Il tutto si basa su due punti:

- la necessità che il responsabile del trattamento **adotti** misure appropriate ed efficaci per attuare i principi di protezione dei dati;
- la necessità di **dimostrare**, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile del trattamento deve fornire la prova di quanto esposto al punto precedente.

Il principio di accountability significa che devo trattare i dati in maniera lecita, corretta e trasparente, devo adeguarmi alla sicurezza, avere tecniche idonee a fronteggiare eventuali attacchi, insomma adottare una serie di misure informatiche fisiche e logiche, adottare comportamenti proattivi, ovvero io come titolare del trattamento mi devo attivare ad attuare quelle tecniche adeguate a prevenire e mitigare i danni. L'accento è posto quindi sulla dimostrazione, sulle prove. Altro punto importante introdotto nel GDPR è il Data protection by default and by design, questi concetti vengono introdotti dalla necessità di andare a sviluppare meccanismi, sistemi e normative che siano progettate e pensate già per essere compliant con il GDPR e quindi con un concetto rispettoso di privacy. I concetti vengono espressi in due punti che ne catturano l'idea:

- Necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
- Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

L'approccio **proattivo** è forse il modo migliore di risolvere il tema dell'essere **Accountable** richiesto dalle norme regolamentari. Essere proattivi è in fondo lo stesso atteggiamento che un'altra norma già presente nel DLgs n. 196/2003 richiedeva e imponeva con l'art. 15 e che oggi, nel regolamento sembra essere presente nell'art. 5: *l'aver fatto e il poter dimostrare di aver fatto tutto il possibile per evitare il danno*. Essere proattivi è il necessario atteggiamento da adottare per non rispondere in futuro di un danno derivante da trattamento dei dati personali attraverso la dimostrazione (**inversione dell'onere della prova**) di aver fatto tutto il possibile per evitarlo. Tale atteggiamento è richiesto al titolare del trattamento dei dati dalle norme regolamentari (es: data breach, misure adeguate di sicurezza) proprio nella fase privacy by design. Anche nelle successive fasi dell'analisi dei rischi, quando il danno è solo un'ipotesi da prevedere, occorre anche in questa fase saper agire in anticipo per far fronte ad una situazione futura anche solo possibile, ipotetica, probabile. Significa avere il controllo e far accadere le cose piuttosto che adattarsi a una situazione o attendere che qualcosa accada per poi porvi rimedio. Responsabilizzarsi non è certamente l'aver adempiuto soltanto agli obblighi di legge. Vuol dire avere un atteggiamento proattivo che non si esaurisce nel semplice adempimento normativo (conformità delle attività di trattamento con il regolamento come reca il considerando 74) e nel dare prova solo di questo adempimento ma ad esempio, anche "**dimostrare l'efficacia delle misure**", rendicontare come si è proceduto e con quali metodologie a definire le misure di sicurezza. Anche in caso di violazione tale atteggiamento, se correttamente rendicontato, può determinare (ex art. 83 del GDPR) da parte dell'Autorità di controllo nel calcolo e nella dosimetria della sanzione eventualmente da applicare, una condizione di favore in capo al titolare che ha saputo attenuare i rischi fino ad un certo limite e l'ha saputo dimostrare. Nell'ambito della sicurezza informatica, l'accountability è anche la capacità di un titolare attraverso il proprio modello privacy di dimostrare attraverso l'audit delle tracce e dal sistema di autenticazione (login) di aver adempiuto agli obblighi previsti dalla normativa in modo sufficientemente anticipatorio di possibili eventi dannosi o critici. Di aver previsto misure organizzative e tecniche rapportate al caso concreto del trattamento ma in grado di essere adatte e adeguate ad una serie sufficientemente ampia di rischi calcolati. Il criterio interpretativo del nesso è sempre **ex ante** in concreto e mai **ex post**. Nessuna norma e non certo il criterio di cui parliamo può spingersi fino a dover dimostrare l'impossibile, il caso fortuito o la forza maggiore o l'evento raramente verificabile. Come in ogni cosa occorre approcciarsi al concetto anche con un po' di buon senso per evitare che la soglia di anticipazione, di previsione e di rendicontazione retroceda all'infinito e diventi impossibile o quasi. Saper anticipare il verificarsi di situazioni critiche, l'accadimento di eventi rischiosi possibili o molto

probabili e trovare soluzioni che, ex ante in concreto, forniscano un certo margine di sicurezza, significa essere **accountable**.

3 SOGGETTI DEL TRATTAMENTO E MODELLO ORGANIZZATIVO

Si è già discusso a fondo la figura del **titolare del trattamento** nel capitolo precedente ma in una realtà amministrativa ci sono diverse figure che, assieme al titolare, devono essere incaricate, previste e regolarizzate al fine di redigere un modello organizzativo adatto e responsabile dell'amministrazione dei dati all'interno dei sistemi. Il primo passo da compiere per una corretta applicazione della normativa è una corretta individuazione dei soggetti che trattano i dati. Da una parte mettiamo il **soggetto passivo**, ovvero gli **interessati** *(la persona fisica alla quale i dati si riferiscono*), mentre dall'altro lato abbiamo quelle figure che compiono raccolta, conservazione, diffusione ecc. del dato. La prima figura importante è il titolare del trattamento. Nel caso dell'università per esempio, il titolare del trattamento è l'università stessa. Accanto al titolare si possono verificare casi di contitolarità del dato, ovvero *dove più soggetti agiscono sullo stesso piano*. I dati vengono trattati dai cosiddetti soggetti del trattamento ed è quindi necessario individuare tali questi soggetti ovvero:

- Titolare del trattamento
- Contitolari del trattamento
- Responsabile del trattamento
- Eventuale sub-responsabile del trattamento
- Responsabile della protezione dei dati (RPD/DPO)
- Soggetti istruiti/autorizzati (Incaricati)
- Amministratori di sistema

3.1 CONTITOLARI DEL TRATTAMENTO

Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento**. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento (art. 26).

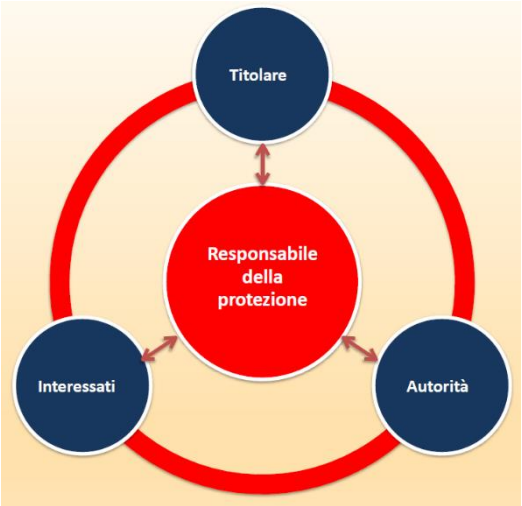
3.2 RESPONSABILE DEL TRATTAMENTO

(art. 28): «*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a **responsabili del trattamento** che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*». C'è la necessità di avere una figura intermedia tra titolare e le persone fisiche che trattano i dati. Il vecchio ordinamento prevedeva il **responsabile interno**. Questa figura fu abolita dal legislatore europeo, anche se in Italia ancora esiste. Questa figura intermedia procede alla nomina dei soggetti attraverso la **lettera di incarico**, che specifica cosa uno può fare con i dati e quali dati può trattare. Il nostro legislatore ha eliminato l'articolo 29 del codice privacy e ci troviamo quindi senza il responsabile del trattamento. Successivamente è stato reinserito con il nome di **referente per la protezione dei dati**, ma con le stesse funzioni di prima. L'incaricato del trattamento può essere solo una persona fisica. Quando un soggetto esterno tratta i nostri dati tale soggetto va responsabilizzato concludendo un contratto di esternalizzazione. Questo contratto però non ci basta, e accanto al contratto lo nomino responsabile del trattamento.

Abbiamo quindi il responsabile interno (il referente) e poi il responsabile esterno (figura alla quale affidiamo compiti e attività che dovremmo fare noi). Può un responsabile del trattamento nominare un sub-responsabile esterno? Può farlo se previsto da contratto, purché dia preventiva comunicazione al titolare del trattamento. Con il vecchio codice, un responsabile non poteva a sua volta nominare un altro responsabile, ma poteva solo il titolare del trattamento. Il responsabile del trattamento non ricorre a un altro responsabile senza previa

autorizzazione scritta, specifica o generale, del titolare del trattamento. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

3.3 RESPONSABILE DELLA PROTEZIONE



La figura del **responsabile della protezione** dei dati è una figura importante in quanto deve rispondere al titolare del trattamento, e nel confronto del quale **conserva una propria autonomia**, e inoltre ha la possibilità di interfacciarsi con autorità. Il nominativo del responsabile con i suoi contatti deve essere inviato all'autorità garante, in quanto se dovesse succedere qualcosa verrebbe subito contattato il responsabile della protezione. L'RPD deve avere competenze giuridiche, capacità relazionali, capacità di comprensione degli aspetti tecnici, conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, conoscenza della disciplina di settore e del contesto nel quale opera il titolare. La responsabilità di garantire ed essere in grado di dimostrare l'osservanza della normativa ricade sul titolare/responsabile del trattamento.

3.4 SOGGETTI ISTRUITI/AUTORIZZATI

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 29) .

3.5 AMMINISTRATORE DI SISTEMA

È colui il quale ha le *"chiavi di casa"* del sistema, colui che ha la massima comprensione del domicilio informatico. Viene introdotta questa figura nel 2008 ed I primi ad individuare questa figura furono gli operatori telefonici, dei servizi internet e l'anagrafe tributaria; questo perché sono soggetti che trattano dati potenzialmente sensibili. Questa figura è molto importante in quanto all'interno di queste compagini hanno un potere illimitato, che potrebbero sfuggire a qualsiasi controllo. **Il garante** si è posto quindi il problema di regolarizzare tale figura, ovvero elevando la sicurezza dei sistemi tracciando comunque l'attività che compie l'amministratore di sistema (in quanto bisogna avere cognizione di ciò che si fa nel sistema informatico). Bisogna prima di tutto evitare i rischi di abuso dei privilegi connessi alla funzione. Questi limiti nascono dal fatto che è una figura che gode di alti privilegi di accesso al sistema e quindi comporta maggiori rischi potenziali. Proprio per questi motivi la normativa europea ha previsto una definizione più completa di tale figura

D.P.R. 318/99	**GDPR**
Amministratore di sistema il soggetto al quale è conferito il compito di sovraintendere alle risorse del sistema operativo di un elaboratore	Comprende non solo figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ma anche altre figure

o di un sistema di banca dati e di consentirne l'utilizzazione	equiparabili dal punto di vista dei rischi relativi alla protezione dei dati: amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e amministratori di sistemi software complessi

In alcuni casi, la figura dell'amministratore di sistema costituisce un aggravante rispetto al **codice penale.** Altra figura che le amministrazioni dovrebbero prevedere è il **responsabile per la transizione al digitale**, figura che deve guidare il passaggio definitivo dalla carta al bit.

4 ADEMPIMENTI DEL TITOLARE

Nel rispetto del principio di **accountability**, il titolare del trattamento ha l'obbligo di adempire a determinate mansioni quali:

Acquisizione del consenso da parte dell'interessato e casistica di esonero dal relativo obbligo (CAPO II – artt. 6 e 7) Ciascun titolare deve distinguere i casi in cui per eseguire un trattamento è richiesto il (previo) consenso dell'interessato, da quelli in cui non è necessario acquisirlo. La richiesta del consenso deve essere presentata in modo distinto da altre richieste, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Quando per un trattamento è necessario il consenso, il titolare deve essere in grado di dimostrare che il consenso è stato effettivamente prestato.
Trasparenza nella gestione dei trattamenti (CAPO III – art. 12) Il titolare è obbligato ad adottare misure appropriate per fornire all'interessato tutte le informazioni/comunicazioni relative ai trattamenti gestiti dalla propria organizzazione, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Il titolare è tenuto ad agevolare l'esercizio dei diritti da parte dell'interessato e, in particolare, a fornire un riscontro alla richiesta del medesimo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della medesima (prorogabile di due mesi ove necessario, tenuto conto della complessità e del numero delle richieste).
Informativa all'interessato (CAPO III – artt. 13 e 14) Adempimento basilare per qualsiasi titolare, si giova necessariamente di una buona capacità di analisi (in particolare) dei flussi dei trattamenti. L'informativa richiesta dal Regolamento UE è più ricca di informazioni di quella attuale e la sua redazione è operazione niente affatto banale: per esempio, il titolare deve esplicitarvi il periodo di conservazione dei dati personali, ovvero i criteri utilizzati per determinare tale periodo. Non in ultimo, il linguaggio dell'informativa deve essere semplice e chiaro. Si distinguono le due fattispecie in cui la comunicazione delle informazioni è da correlare alla raccolta dei dati presso l'interessato ovvero presso un soggetto diverso.
Misure di sicurezza adeguate (CORPO IV art. 24 e 32) Il titolare del trattamento deve adottare misure tecniche e organizzative adeguate al fine di garantire, ed essere in grado di dimostrare, la conformità del trattamento al Regolamento. Ciò tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. Le predette misure devono essere periodicamente riesaminate e aggiornate.
Privacy by design (fin dalla progettazione) CORPO IV – art. 25.1 All'atto del trattamento e della determinazione dei mezzi dello stesso, il titolare adotta misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati. Nel fare ciò deve tener conto delle specifiche caratteristiche del trattamento e dei connessi profili di rischio per i diritti e le libertà delle persone fisiche
Privacy by default (per impostazione predefinita) CORPO IV – art. 25.2

Il titolare del trattamento attua misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ciascuna finalità del trattamento. Obbligo che vale per la quantità dei dati raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità ai dati stessi.

Contitolarità del trattamento (CORPO IV – art. 26)
Nel caso in cui due o più titolari operano come contitolari del trattamento (determinando congiuntamente finalità e mezzi del medesimo), concordano in modo trasparente, mediante un contratto, la ripartizione delle responsabilità del trattamento, con particolare riguardo all'esercizio dei diritti degli interessati e ai connessi obblighi informativi. Il contenuto essenziale dell'accordo deve essere messo a disposizione degli interessati.

Nomina del Rappresentante del titolare (CORPO IV – art. 27)
Laddove si applichi l'art. 3.2 (trattamento di dati personali relativi ad interessati che si trovano nell'Unione da parte di titolare/responsabile non stabilito nell'UE), il titolare/responsabile designa per iscritto un proprio rappresentante nell'Unione. Il rappresentante è l'indefettibile interlocutore della competente autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

Nomina del Responsabile del trattamento (CORPO IV – art. 28)
Il titolare può nominare un responsabile che effettui il trattamento per suo conto. Il titolare ha la responsabilità di scegliere per tale incarico un soggetto/organismo che presenti garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate. Il Regolamento stabilisce un numero cospicuo di requisiti minimi di contenuto del contratto tra titolare e responsabile del trattamento.

Obbligo di istruzione da parte del Titolare (CORPO IV – art. 29)
Il titolare del trattamento deve previamente istruire tutti coloro che siano autorizzati ad accedere ai dati personali, compreso il responsabile del trattamento.

Adozione del Registro delle attività di trattamento (CORPO IV – art. 30)
Il titolare del trattamento con almeno 250 dipendenti o che, anche al di sotto di tale soglia dimensionale, deve obbligatoriamente effettuare un trattamento che possa presentare un rischio per i diritti e le libertà degli interessati che non sia occasionale o che includa dati sensibili, genetici, biometrici, giudiziari. Cuore del documento è una mappa dettagliata di tutti i trattamenti effettuati dall'organizzazione del titolare.

Obbligo di cooperazione con l'autorità di controllo (CORPO IV – art. 31)
Il titolare è tenuto a cooperare con l'autorità di controllo, quando quella gliene faccia richiesta.

Notificazione di una violazione dei dati (CORPO IV – art. 33)
Rientra tra gli obblighi del titolare anche la notifica all'autorità di controllo (Garante) senza ingiustificato ritardo – e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza -, di ogni violazione della sicurezza dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche.

Comunicazione di una violazione dei dati all'interessato (CORPO IV – art. 34)
Quando la violazione della sicurezza dei dati presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve darne notizia all'interessato senza ingiustificato ritardo. La norma fissa i requisiti di contenuto della comunicazione, che deve essere redatta con un linguaggio semplice e chiaro. Altresì la norma individua i casi in cui la detta comunicazione non è richiesta (per semplicità, quando il titolare ha adottato misure tali da scongiurare il rischio o quando la comunicazione richiederebbe sforzi sproporzionati).

Redazione della Valutazione d'impatto sulla protezione dati e consultazione dell'autorità di controllo (CORPO IV – artt. 35 e 36)
Si tratta di un ulteriore adempimento che grava sul titolare che debba iniziare un trattamento molto rischioso per i diritti e le libertà delle persone fisiche. Ciò si può verificare, in particolare, quando sia implicato l'uso di nuove tecnologie, ovvero in considerazione di altre caratteristiche (natura, oggetto,

contesto, finalità) del trattamento. Quando la valutazione di impatto indichi che il trattamento presenta un rischio elevato, prima di procedere al trattamento il titolare è tenuto a consultare l'autorità di controllo.
Nomina di un Responsabile della Protezione dei Dati (Data ProtectionOfficer – DPO) (CORPO IV – artt. 37 e 39) Il DPO dev'essere nominato obbligatoriamente nell'ipotesi in cui il titolare del trattamento: a) è autorità/organismo pubblico (eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali); b) effettua trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; c) effettua come attività principali trattamenti su larga scala di dati sensibili, genetici, biometrici, giudiziari. Ha compiti di informazione, formazione, consulenza e sorveglianza dell'adempimento della disciplina privacy ed è anche interlocutore dell'autorità di controllo.
Adesione a codici di condotta/sistemi di certificazione (CORPO IV – artt. 40, 41 e 42) Sono adempimenti volontari del titolare mediante i quali si possono implementare misure di sicurezza dei trattamenti e si può dimostrare la conformità delle attività di trattamento ai requisiti stabiliti dal Regolamento.
Obbligo di risarcimento del danno (CAPO VII) Il titolare è tenuto a risarcire il danno materiale o immateriale cagionato da una violazione del Regolamento eccetto nel caso in cui dimostri la non imputabilità per l'evento lesivo.

Abbiamo visto come il GDPR imponga diversi obblighi al titolare del trattamento al fine di garantire una corretta comprensione e applicazione della normativa. Per una trattazione più approfondita di alcuni dei più importanti adempimenti che gravano sul titolare, si andranno a definire alcuni aspetti del:

- Mantenimento dei registri delle attività di trattamento (art. 30)
- Valutazione di impatto e consultazione preventiva (artt. 35-36)
- Sicurezza dei dati personali (artt. 32-34)
- Notifica delle violazioni (art. 33)

4.1 REGISTRO DEI TRATTAMENTI

Tutti i **titolari** e i **responsabili di trattamento**, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Questo registro è la fotografia di come vengono trattati i dati in un determinato ambiente. Il titolare del trattamento riassume in una tabella quelli che sono i dati che tratta, le modalità, le misure di sicurezza che implementa per proteggere i dati, e fornisce un quadro generale sulle operazioni compiute sui dati, con misure e contro misure per proteggere i dati personali. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Il contenuto del registro del titolare deve contenere i dati di contatto delle figure che trattano il dato, quindi del titolare del trattamento, dell'RPD e dell'eventuale co-titolare. Va inoltre indicato il motivo per il quale si tratta il dato, e la base giuridica del trattamento. Vengono poi indicati i soggetti interessati, e si indica quali tipi di dati si hanno delle persone. Categorie destinatari e trasferimenti dei dati. Bisogna poi indicare i termini di cancellazione, ovvero un dato deve essere cancellato una volta che non serve più. Ad oggi il dato può essere tenuto fino a 36 mesi, prorogati ovviamente in caso di inchieste in corso. Vi sono inoltre misure tecniche e organizzative, ovvero come mi organizzo per gestire i dati e proteggerle. Ci sono poi contenuti che possono arricchire il registro, come la possibilità di menzionare una determinata certificazione, così come l'adesione ad un codice di comportamento o un codice di condotta. Un titolare può avere un registro come titolare del trattamento e uno come responsabile del trattamento, per esempio, l'università ha il suo registro come titolare del trattamento, ma se dovesse collaborare con un'altra università per un progetto, dovrebbe anche compilare un registro del responsabile del

trattamento. Registro del responsabile: molto più semplificato di quello del titolare. La legge non dice come deve essere tenuto questo registro. Il registro dei trattamenti non è uno strumento statico ma dinamico in quanto cambia continuamente per adattarsi alle novità di un'amministrazione.

4.2 GESTIONE DEL RISCHIO

la gestione del rischio implica il fare un'**analisi implementativa**, classificare i dati, calcolare quali sono i dati più a rischio (password per le transazioni, strumenti per il trasferimento di fondi ecc). Rischio è da intendersi relativamente di impatti negativi sulle libertà e i diritti degli interessati (si vedano cons. 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di **valutazione** (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati adottate dal Gruppo, Art. 29). All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento. La valutazione di impatto si conclude con una relazione finale in cui si indicano finalità, quali dati tratto, quali sono le misure amministrative ecc. Il titolare può decidere se andare avanti o meno in quanto si assume le responsabilità.

4.3 MISURE DI SICUREZZA

sono tra gli adempimenti principali richiesti al titolare del trattamento. L'articolo 24 quando fa riferimento alle misure organizzative più idonee e adeguate ai rischi, si riferisce anche all'adozione da parte del titolare del trattamento di misure di sicurezza adeguate. Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, p. 1). Per lo stesso motivo, non sussistono dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "**minime**" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, l'autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti. la misura di sicurezza va valutata in relazione al tipo di dato che vogliamo trattare e in base alle modalità del trattamento che vogliamo porre. Se si trattano dati sulla salute o sull'orientamento sessuale o dati genetici, sono molto più importanti di altri tipo di dati e devono essere protetti con misure di sicurezza molto forti. I dati genetici quindi, anche se sono conservati in un database non connesso alla rete, devono essere comunque, come minimo, cifrati. La nuova normativa informa anche sul come deve avvenire la circolazione, la comunicazione, la diffusione dei dati. Per esempio, la comunicazione di dati sanitari da una struttura all'altra deve essere tramite posta elettronica certificata. Altro principio fondamentale oltre la natura del dato, per valutare l'adeguatezza del dato, è l'aggiornamento della misura. Il dato non solo deve essere costantemente aggiornato (articolo 5), anche i sistemi di sicurezza informatici devono essere costantemente aggiornati ove tali aggiornamenti devono essere fatti allo stato dell'arte.

4.4 NOTIFICA DELLE VIOLAZIONI

Tutti titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. La violazione del dato può essere dal punto di vista **logico** (accesso abusivo al sistema informatico), oppure un qualcosa di **materiale** come la perdita dello smartphone con sincronizzata magari l'e-mail istituzionale. Questa perdita espone a rischio non solo il possessore ma anche verso terzi, verso le persone con cui abbiamo scambiato messaggi, file in Google drive ecc. Violazione dei dati sono all'ordine del giorno, come la perdita di un documento, o di una cartella con dati degli studenti ecc. Per evitare però di affollare di notifiche l'autority, si è pensato di segnalare solo le violazioni capaci di ledere i diritti della persona. Il garante, una volta ricevuta la segnalazione, manda gli ispettori. Quando vi è una violazione del dato vi è anche il problema di informare gli interessati. Se per esempio viene bucata una sezione della banca dati dell'università in cui sono presenti informazioni relative a persone disabili che hanno diritto a determinati sostegni, vanno subito avvisati che i loro dati sono stati violati. Si potrebbe addirittura richiedere un risarcimento dei danni in quanto magari non erano state adottate misure di sicurezza opportune. I dati sanitari devono essere sempre inviati in forma criptata dalla posta elettronica certificata, o al massimo avere un sistema basilare di autenticazione tramite il quale accedere con user-id e password. L'intervento delle autorità di controllo sarà principalmente "**ex post**", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior-checking, sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia, con eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Alle autorità di controllo, e in particolare al Comitato europeo della protezione dei dati spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici.

5 CONCLUSIONI

Arrivati alla fine della tesina possiamo trarre delle conclusioni in merito al nuovo regolamento. Sappiamo che ogni qualvolta si lavora e ci si mobilita per la stesura di nuovi **diritti** e **doveri** c'è sempre una necessità a cui far fronte. In questo caso il **GDPR** viene introdotto proprio per far fronte a questo fenomeno di condivisione e digitalizzazione di tutto ciò che ci circonda. Il **Web** è la necessità che il mondo ha manifestato negli ultimi anni, la necessità di avere un portale sul mondo. Viviamo in una società sempre più disposta a condividersi e mostrarsi senza alcun limite, ma poche persone capiscono cosa diamo in cambio di tutto ciò. Il **dato**, ora più che mai è qualcosa che ci rappresenta, che ci identifica e ci schedula. Le informazioni che generiamo sono sempre più complesse e piene di significato per gli occhi attenti, di questi occhi ce ne sono tanti: persone/aziende interessate alle nostre abitudini, al nostro modo di pensare ed agire. La normativa è un primo passo verso la regolamentazione di tali soggetti, ed è anche un primo **segnale** molto importante che l'intera comunità europea ha dato ai grandi colossi dell'informazione in quanto denota che il concetto di privacy non è sottovalutato, anzi è tenuto ben in considerazione da tutto l'apparato giuridico europeo. Come spesso ripetuto a lezione, i segreti sono necessari e sono quelle informazioni che caratterizzano la parte più intima di una persona e che si riflettono negli usi, gli hobby ed i pensieri che mostriamo (e non mostriamo) al mondo intero. Proprio per questo tutti insieme (ognuno nel suo ambito) abbiamo il dovere di proteggere quello che forse è, ai giorni d'oggi, il più importante *"oggetto"* che possediamo: **il dato**.