UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"*ESISTE ANCORA LA PRIVACY? DAL D.LGS. 196/2003 AL REGOLAMENTO UE 679/2016: COSA CAMBIA IN AMBITO AZIENDALE?*"

RELATORE:

CH.MO PROF. FILIPPO VIGLIONE

LAUREANDO: IVAN ALDERISIO

MATRICOLA N. 1090224

ANNO ACCADEMICO 2016 – 2017

Indice

Capitolo 1-Privacy: significato, valore, diritto. **p.3**

Capitolo 2-Dal D.Lgs. 196/03 al Regolamento UE 679/16. **p.10**

La disciplina italiana **p.10**

Il Garante nazionale **p.14**

Il nuovo orizzonte europeo **p.16**

Capitolo 3-Cosa cambia in ambito aziendale? **p.27**

Lo Statuto dei lavoratori **p.28**

La sicurezza dei dati **p.29**

La "nuova" sicurezza dei dati **p.30**

Le principali novità "aziendali" del Regolamento: *privacy by design, privacy by default,* principio di *accountability* **p.32**

Il DPO **p.35**

Conclusioni **p.38**

Bibliografia **p.40**

Capitolo 1

Privacy : significato, valore, diritto.

L'informazione è potere. Chiunque al giorno d'oggi detenga più informazioni possibili riguardanti un altro o tanti altri individui, ha potere su quel singolo o addirittura su quella moltitudine: un potere che giunge attraverso il controllo della "preda" e che poi porta al condizionamento di quest'ultima, poiché per dirla alla orwelliana maniera *chi controlla il passato, controlla il futuro*[1], il che è accettabile e privo di rischi, bensì pieno di benefici se il "controllante" è allo stesso tempo il "controllato", ma è pericoloso e talvolta catastrofico se invece il primo differisce dal secondo.

Quando, dunque, abbiamo permesso che quanto appena descritto sia potuto divenire realtà? C'era una volta un tempo in cui i passeggeri si imbarcavano sugli aerei senza essere perquisiti, una volta in cui il significato della parola "hacking" e da lì "hacker" (soprattutto per i non anglosassoni) era totalmente sconosciuto, se si fa riferimento alla più pericolosa accezione che questi termini hanno assunto in tempi recenti.

Ormai l'ubiquità del *Grande Fratello*[2] non fa più notizia.

Sorveglianza elettronica, circuiti chiusi nei luoghi pubblici e/o lavorativi, controllo dei telefoni cellulari e a cascata delle comunicazioni, stupefacenti moltiplicazioni di dati privati a causa di piattaforme di social networking (Facebook, Twitter, YouTube) ormai sono realtà quotidiane; tutto ciò, però, banalizza il significato che necessita di essere attribuito alle questioni legate alla privacy.

Già, privacy, punto chiave e dolente del dilemma, una primaria esigenza di proteggere, soprattutto ma non solo, informazioni particolarmente delicate: la sua violazione non è altro che una effettiva o potenziale perdita di controllo su questioni personali inutilmente rese pubbliche, attraverso magari un semplice clic sullo smartphone, oppure spiate.

Se infatti da una parte, come avviene nella maggior parte dei casi, i responsabili della violazione della privacy sono proprio gli stessi soggetti che successivamente lamentano del pericolo relativo alla diffusione delle informazioni in questione, dall'altra tali responsabili

---

[1] ORWELL, G., 1949. *1984.* Milano: Mondadori.

[2] George Orwell nel suo romanzo distopico "1984" denominava "*Grande Fratello*" il soggetto che simbolicamente teneva ciascun individuo sotto controllo.

possono anche essere soggetti terzi che “vigilano” sulla vita, sulle attività e sugli interessi dei “controllati”, per fini più o meno pacifici, ma con mezzi decisamente invasivi.

Si sta sicuramente facendo riferimento alla sorveglianza degli Stati sovrani nei confronti dei propri cittadini, ma non solo.

Negli anni anche molto recenti, sono presenti numerosissimi esempi di controlli effettuati dalle agenzie governative statali, giustificati spesso da obiettivi o finalità non proprio onorevoli.

Non molto tempo fa, in un susseguirsi di dichiarazioni, un consulente governativo statunitense Edward Snowden ha letteralmente rovesciato un vaso di Pandora: l’enorme estensione della sorveglianza gestita dalla National Security Agency (NSA) statunitense, rea di aver raccolto i dati telefonici di decine di milioni di cittadini[3]. E’ plausibile ritenere che la motivazione celata dietro questo tipo di attività governativa sia meramente la sicurezza della nazione o c’è dell’altro? Fortunatamente non è questa la sede idonea a dirimere tale dubbio.

Ciò che rimane però è la preoccupazione, o l’amara rassegnazione una volta appreso che potenzialmente qualunque tipo di comunicazione potrebbe essere controllata e da lì che la privacy di ciascuno potrebbe essere violata.

Legittimi timori, questi, che hanno avuto ulteriore riscontro a causa di rivelazioni di diversi importanti operatori nell’ambito della telefonia mobile nel mondo riguardo la reale, concreta possibilità da parte di disparate agenzie governative di setacciare tutte le comunicazioni che viaggiano sulla rete.

Questa appena descritta, dovrebbe essere la violazione della privacy per così dire “genuina” , compiuta dallo Stato per tutelare la sicurezza, almeno in teoria, dei propri cittadini.

Viceversa esistono dei sistemi funzionali a scardinare la sicurezza delle informazioni private come intercettazioni o “cimici”, molto semplici da attuare anche da parte di individui che nulla hanno da spartire con enti pubblici, statali o agenzie governative poiché semplici malintenzionati che sfruttano le informazioni ottenute di nascosto a discapito dei violati, per ottenere un qualche profitto o beneficio.

Tuttavia, facendo qualche passo indietro, l’attività di controllo e dunque implicitamente di violazione della privacy può essere addirittura agevolata quando essa è ritenuta astrattamente lecita: consultare motori di ricerca o mappe tramite GPS (Global Positioning System) sul web, navigare in Internet, inviare documenti tramite mail sono attività che certamente sono

---

[3] WACKS, R., 2016. *Privacy Una sintetica introduzione.* 1^ ed. Pescara: Monti & Ambrosini editori.

entrate nel "patrimonio" di chiunque, attività ordinarie e totalmente di routine, ma che contemporaneamente possono anche essere oggetto di facile controllo da chi si trova dall'altra parte della barricata, al di là dello schermo. Ciò può avvenire in modo limpido attraverso politiche tecnologiche come *cookies*, non biscotti edibili, bensì tecnologie che permettono di memorizzare le attività compiute su uno specifico computer, oppure in modo malevolo, illecito attraverso malware, spyware, cavalli di Troia e così via discorrendo.

Il Grande fratello vi guarda![4] Una minaccia, una intimidazione che rende ancora più consapevoli di essere osservati, di essere controllati e ancor più di essere desiderosi del ripristino di un valore fondamentale che è quello della privacy.

Innanzitutto un' idea, questa, che consiste nel desiderio inconscio di ciascun individuo di essere lasciato solo, libero dal giudizio o da altro tipo di inibizioni, costrizioni derivanti dall'essere osservati.

Ma chi o cosa potrebbe controllare le attività, le azioni degli altri in modo così gravoso, così opprimente da compromettere il sereno svolgimento delle stesse da parte degli "osservati" ?

Di primo acchito, riprendendo il discorso di qualche riga fa, verrebbe da rispondere a questa domanda con "malintenzionati" o magari "semplici curiosi": soggetti comunque tutti posti sullo stesso piano dello "spiato".

In realtà molto spesso, come già accennato in precedenza, il controllo deriva da un individuo posto in una qualche posizione di sovraordinazione rispetto alla vittima: da qualcuno che in termini ampi e generici potrebbe essere assimilato alla definizione di "pubblico" da cui è possibile giungere ad ambiti più marcati e specifici come possono esserlo lo Stato, il datore di lavoro, un ente pubblico, un qualche tipo di autorità e così via.

D'altronde il desiderio di affermazione di una sfera cosiddetta privata presuppone implicitamente l'esistenza di una sfera, al contrario, pubblica: non a caso gli antichi Romani percepivano ciò che oggi si definisce privacy come semplicemente un temporaneo riposo dalle fatiche della vita nel contesto della *res publica.*

Traslando dunque il significato ai giorni nostri, una identificazione e una valorizzazione di un contesto privato libero dall'occhio vigile in primis dello Stato.

Un valore quindi, quello della privacy ,che sicuramente non è di recente acquisizione, di recente genesi, anzi ha radici ben più profonde e lontane nel tempo.

---

[4]ORWELL, G., 1949. *1984.* Milano: Mondadori. Pag.2.

La privacy, a questo punto, può essere facilmente intesa come una sorta di guscio al cui interno potersi liberamente esprimere, manifestare la propria creatività, costruire rapporti di fiducia, amicizia…, il tutto promuovendo l'autonomia personale e permettendo anche una sorta di rilassamento emotivo, senza alcun tipo di inibizione o impedimento.

Tuttavia questo eccessivo lassismo, questa oasi della libertà va a scontrarsi con quelle che potrebbero essere altre necessità del "pubblico" a tutela del "privato": questioni legate alla sicurezza, alla identificazione di soggetti pericolosi potrebbero essere rese più difficoltose da una eccessiva difesa del santuario costruito in nome della privacy.

Per non parlare del contrasto che potrebbe sorgere con aspetti legati all'etica, alla moralità dal momento che la privacy potrebbe essere tratteggiata anche come un principio di autodeterminazione fondato sulla libertà di compiere, indisturbati, attività private di qualunque genere.

Problematiche, queste, discendenti dal fatto che manca una definizione univoca del concetto in questione, che sotto una certa luce può consistere nuovamente in un principio di autodeterminazione[5], ma questa volta autodeterminazione della estensione della diffusione di proprie informazioni comunicate ad altri. Ossia, da un lato, è sicuramente possibile rendere partecipi altri delle proprie attività conoscendo a priori quei soggetti cui si estendono le informazioni, ma dall'altro lato questa percezione di controllo della destinazione delle suddette informazioni è limitata perché non è altresì possibile controllare in un secondo momento come esse viaggino e presso quali contesti giungano al di là di quei magari pochi individui cui le informazioni sono state diffuse.

Si passa a questo punto da un diritto alla riservatezza ad un diritto del controllo dei propri dati, della diffusione degli stessi.

Proprio a questo riguardo la crescente propagazione sin dagli anni '60 dell'informazione su larga scala supportata dai progressi tecnologici dei computer ha portato ad un sempre più elevato fenomeno di circolazione di dati personali, in modo del tutto incontrollato.

L'informazione non è più soltanto potere, ma è diventata un grande business.

A metterci una pezza, per così dire, sono state le varie regolamentazioni, europee tra le altre, a tutela di tali dati, basate sul principio che questi ultimi debbano essere raccolti nei limiti delle lecite finalità per cui siano stati collezionati o altrimenti anche per altri obiettivi previo un consenso più ampio dell'interessato.

---

[5]WESTIN, A. F., 1967. *Privacy and freedom.* New York: Atheneum. Pag.7

Il punto di partenza per ogni tipo di regolamentazione in merito è, però, la definizione di "dato personale": ogni tipo di informazione concernente persone fisiche identificate o identificabili in base a specifiche caratteristiche.

La protezione dei dati personali funge da scudo per la privacy, anche se in realtà la relazione tra questi due temi non è immediatamente chiara dal momento che i due concetti sono complementari e non sinonimi.

Essi spesso si sovrappongono e la tutela della privacy è invocata come una sorta di sostegno alla difesa dei dati personali, i quali possono riguardare sia informazioni non necessariamente private, sia allo stesso tempo altre di natura effettivamente non pubblica.

Nonostante, a questo punto, la mancanza di univocità del concetto di privacy e anche la possibilità di commistione con la definizione relativa ai dati personali è necessario constatare che contemporaneamente a queste "lacune" da un punto di vista prettamente terminologico ed eziologico, sin dal XIX secolo la privacy (in senso generale includente anche l'aspetto dei dati personali) è stata riconosciuta come un bene giuridicamente protetto, originariamente nei sistemi giuridici caratterizzati da *common law*, i quali prevedevano che la legge riconoscesse l'importanza dei bisogni intellettuali e spirituali dell'uomo.

Il diritto alla privacy, quindi, nasce come un diritto alla riservatezza, il diritto di "essere lasciati soli"[6].

Successivamente, un altro esempio in merito può essere l'orientamento continentale europeo basato sul concetto di "diritto alla personalità" (*...ciascuno deve avere il diritto al libero sviluppo della propria personalità...*- Legge Fondamentale della Repubblica Tedesca). Ulteriori approcci possono essere ricavabili in un'ottica internazionale dalla Dichiarazione Internazionale dei Diritti dell'Uomo e dalla Convenzione Internazionale sui Diritti Civili e Politici dove appunto, in estrema sintesi, *nessuno deve subire un'interferenza arbitraria o illegale nella propria privacy, famiglia, domicilio...*

La domanda a questo punto non può che essere una sola: sono sufficienti queste misure normative a garantire appieno la privacy e tutto ciò che ne consegue?

---

[6] Precisamente l'atto di nascita della privacy come un vero e proprio bene, fu idealmente siglato da un famoso articolo scritto nel 1890 da Samuel L. Warren e Louis D. Brandeis, due avvocati bostoniani che per la prima volta misero a confronto il diritto dell'informazione con quello di riservatezza, e pubblicato dalla rivista giuridica Harvard Law Review.
WARREN, S. L., e BRANDEIS, L.D, 1890. *The right to privacy.* Boston: Harvard Law Review. Disponibile su: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [data di accesso: 16/05/2017].

Di certo, non si può affermare che questo diritto fondamentale sia morto, che sia già arrivata l'ora del suo "requiem", però d'altra parte bisogna allo stesso tempo ammettere che per mantenere viva e vegeta, solida più che mai la privacy, sono necessari continui interventi legislativi e normativi che siano sempre aggiornati ed al passo con i tempi che corrono.

In sostanza per prevenire il "male" della privacy, occorre prima studiarlo, conoscerlo e utilizzarlo a proprio vantaggio, come un vero e proprio antidoto .

Ovviamente il collegamento è intuitivo e porta alla tecnologia: tanto più il progresso tecnologico e l' innovazione aumentano, tanto più grandi ed insidiose saranno le minacce di invasione della nostra sfera privata.

Siamo, al giorno d'oggi, sempre di più dinnanzi ad un bivio: ad una strada che conduce al rispetto e alla tutela della privacy personale e ad un'altra che invece porta al letterale godimento del paradiso tecnologico che viene presentato sempre diverso giorno dopo giorno, anno dopo anno, in costante evoluzione.

Tuttavia intraprendere, percorrere quest'ultima strada non presenta solo dei benefici, anzi ha anche un costo, un prezzo molto elevato, perché per vivere in un mondo colmo di vantaggi tecnologici, bisogna sacrificare qualcosa, rinunciare a qualcosa: quel "qualcosa" è proprio la privacy.

Essa viene progressivamente scalfita dalla crescente e sempre più diffusa accondiscendenza, indifferenza o addirittura apatia che si mutano in un appoggio tacito e silente nei confronti di misure tecnologiche, le quali sono divenute talmente quotidiane da costringere gli utenti a percepirle come indispensabili, assolutamente necessarie.

Fortunatamente, come si accennava in precedenza, la tecnologia può anche presentare una sfaccettatura positiva, un lato più favorevole nei confronti della privacy.

Nel mondo odierno, in un mondo che sembra bearsi dei suoi continui progressi in campo tecnico e scientifico, la sola legge, i soli interventi normativi non sono sufficienti a garantire la massima protezione, o meglio la protezione che un diritto cardine come la privacy dovrebbe meritare, poiché una tutela davvero efficace ha un disperato bisogno anche della tecnologia, contemporaneamente causa e cura della "malattia".

Questa sbalorditiva capacità dello strumento tecnologico per eccellenza, ossia l'Internet, di raccogliere, collezionare, archiviare, trasferire, confrontare una incredibile mole di informazioni genera, senza ombra di dubbio, delle perplessità, dei genuini timori, portando dunque a far percepire la tecnologia come un avversario, come un qualcosa che "invade", ma allo stesso tempo può e deve divenire un alleato.

I nuovi avveniristici metodi investigativi basati proprio su approcci e mezzi innovativi e tecnologici, utilizzati ad esempio dalle forze di polizia o di intelligence, concorrono a raggiungere quello che in teoria dovrebbe essere l'obiettivo primario del plurinominato "pubblico": proteggere la cittadinanza.

E se per fare ciò, è necessario entrare nel "focolare domestico" di ciascun individuo, ben venga: sull'altare della sicurezza collettiva occorre sacrificare qualcosa, una più o meno ampia porzione della propria riservatezza.

Si è quindi pervenuti ad una soluzione? Dato che ormai non è più possibile garantire appieno la privatezza, bisogna davvero accettare una sorta di compromesso, in funzione del quale l'interesse del singolo debba essere parzialmente offerto in sacrificio in nome di un pubblico bene o interesse?

Di sicuro è necessario trovare un equilibrio: la privacy deve essere sì tutelata, ma contemporaneamente deve ammettersi per il bene e la sicurezza collettivi l'esigenza di alleggerire tale tutela, anche e soprattutto per il tramite di mezzi tecnologici, purché nei limiti di quelle stesse leggi e regolamentazioni che hanno il compito ed il dovere di garantire la protezione della privacy.

Il cerchio sembrerebbe venire a chiudersi.

Dunque, scopo di questo elaborato è ricercare le ultime "innovazioni" normative che tutelano la privacy, in qualche modo resuscitando questo valore, descrivendo il nuovo Regolamento, 679/2016, dell'Unione Europea sulla protezione dei dati personali, attraverso anche un excursus sulla precedente disciplina italiana vigente in merito, ossia il decreto legislativo 196/2003 denominato appunto "Codice della privacy" ; un apposito focus sarà inoltre dedicato alle novità normative concernenti i contesti aziendali riguardo tali aspetti.

Un intervento del legislatore comunitario avvenuto dopo ben ventuno anni dall'ultima Direttiva della UE (95/46/CE) proprio in riferimento a tale argomento: tempo intercorso, questo , che sicuramente si è reso necessario, in linea con il discorso tenuto in precedenza, per adattare e in qualche modo plasmare a proprio vantaggio tutte quelle situazioni che potrebbero mettere in pericolo la privacy, come la stessa tecnologia, lo stesso progresso tecnologico.

Disciplina legislativa che quindi si aggiorna tentando di assimilare e comprendere le nuove minacce alla privacy, per sfruttarle a vantaggio della stessa, comunque ponderando non solo le esigenze dei potenziali "controllati" , ma anche quelle delle eventuali controparti (Stato, autorità pubbliche, datori di lavoro…).

Il Grande Fratello vi guarda! Sì, lo sappiamo ma abbiamo anche imparato a difenderci.

Capitolo 2

Dal D. Lgs. 196/03 al Regolamento UE 679/16.

La disciplina italiana

*"*Chiunque ha diritto alla protezione dei dati personali che lo riguardano"[7]. Inciso, questo, che potrebbe facilmente essere considerato un luogo comune o un semplice slogan, oppure potenzialmente assimilabile ad una qualche rivendicazione di utenti privati nell'ambito dell'utilizzo di tecnologie informatiche. Nulla di tutto ciò.

Una definizione, anzi addirittura una semplice frase che nonostante la sua brevità rappresenta il principio cardine su cui si basa l'intera legislazione italiana vigente riguardo la protezione dei dati personali, nonché il primo articolo del Decreto Legislativo 30 giugno 2003, numero 196, denominato per l'appunto "Codice della privacy".

Qualunque trattamento di dati personali deve avvenire nel rispetto dei diritti e delle libertà fondamentali dell'individuo, con una particolare attenzione nei confronti della sua dignità.

Fin qui tutti d'accordo. Ma cosa significa nella sostanza l'espressione "trattamento di dati personali"? Chi è che tratta questi dati e quali sono le informazioni da tutelare contenute in essi? In nostro soccorso, per rispondere a questo *tourbillon* di quesiti, di dubbi, giunge puntuale il Codice poco fa accennato: qualunque operazione o insieme di operazioni automatizzate o meno riguardanti raccolta, registrazione, conservazione, consultazione, elaborazione ed eventuale cancellazione e distruzione di dati è da intendersi come trattamento[8].

I dati, oggetto di tali situazioni, possono essere catalogati in *personali*, se comprendono qualunque informazione relativa a persone fisiche identificate o identificabili anche indirettamente mediante ricorso ad altro tipo di notizie, *sensibili* qualora rivelino l'origine razziale ed etnica, le convinzioni socio-politiche, religiose, filosofiche ecc. e infine *giudiziari* nel caso in cui diffondano informazioni in materia di casellario giudiziale e di anagrafe alle sanzioni amministrative dipendenti da reato.

L'attuale disciplina italiana prevede l'identificazione di tre categorie di soggetti che si occupano del trattamento e di conseguenza della protezione dei dati: *titolare*, *responsabile* ed *incaricato*. Il primo è quel soggetto, sia persona fisica come può esserlo un imprenditore sia

---

[7] Dlgs. 30 giugno 2003, n°196, art.1.

[8] Dlgs. 30 giugno 2003, n°196, art.4.

persona giuridica sotto forma di s.r.l. ad esempio, cui compete l'esercizio di un potere decisionale autonomo sulle finalità, le modalità e gli strumenti relativi alla fruizione di tali dati: il titolare a questo punto ha la possibilità, attraverso una sorta di delega di funzioni, mediante atto scritto di nominare un altro soggetto, il responsabile, che è preposto al trattamento secondo le istruzioni impartite dal primo[9].

A cascata, ora, possono essere nominati sempre per iscritto anche gli incaricati, ossia persone fisiche autorizzate dal titolare o dal responsabile a compiere operazioni concrete di trattamento: delegati di esecuzione per così dire.

I "poteri" di questi soggetti possono riguardare anche dati detenuti all'estero, purché chiunque ne effettui il trattamento sia stabilito nel territorio dello Stato italiano ovviamente.

Fino ad ora, almeno, tutte disposizioni riguardanti il "lato attivo" del famigerato controllo, il lato di chi invade la nostra sfera privata, carpendone dati, perciò la domanda sorge spontanea: e l'altra parte, l'altra faccia della medaglia? Gli interessati, cioè le persone fisiche cui si riferiscono i dati, sono tenuti a subire inermi il trattamento delle loro informazioni? Ovviamente non è così: è prevista tutta una serie di diritti, i quali in qualche modo permettono al soggetto interessato di potersi difendere, qualora ve ne fosse necessità, almeno parzialmente dal trattamento.

Il Codice della privacy prevede in questo ambito (invero molto ampliato dal nuovo Regolamento UE, di cui si parlerà in seguito) che l'interessato possa ottenere l'accesso, chiedendone preventivamente conferma dell'esistenza, ai dati che lo riguardano con indicazione circa la loro origine, le finalità e le modalità del trattamento, gli estremi identificativi del titolare e/o del responsabile e finanche il periodo di conservazione degli stessi. Inoltre è possibile un aggiornamento, una rettifica o qualora ve ne sia bisogno anche una integrazione dei dati, nel caso in cui questi si presentino come lacunosi o errati.

E di gran lunga più importante è il diritto dell'interessato di opporsi, in toto o parzialmente, al trattamento: eccezion fatta, tra gli altri, di casi o situazioni che abbiano la loro genesi in soggetti o autorità pubbliche oppure che siano derivanti da ragioni di giustizia.

---

[9] La caratteristica che accomuna, dunque, titolare e responsabile è che entrambi hanno la responsabilità giuridica del rispetto degli obblighi imposti dalla normativa. Perciò l'uno o l'altro deve essere in grado di rispondere, per la parte di trattamento che lo riguarda, di eventuali violazioni e problematiche.
PIZZETTI, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli. Pag.198.

Parallelamente ai diritti menzionati appena qualche riga fa, i soggetti interessati dovrebbero, almeno in teoria, dormire sonni tranquilli, per così dire, dal momento che l'utilizzo di dati personali deve obbligatoriamente avvenire secondo principi di trasparenza e correttezza: le informazioni devono essere trattate in modo lecito poiché raccolte per scopi legittimi e soprattutto espliciti, non in modo eccedente rispetto alle finalità per le quali sono state collezionate originariamente.

Tutto ciò reso in teoria ancora più adamantino, dalla promozione di codici di deontologia e di buona condotta pubblicati a cura del Garante della privacy (figura di primo rilievo, cui sarà dedicata una specifica parentesi successivamente).

I due pilastri di trasparenza e correttezza che in qualche modo dovrebbero guidare la mano di chi si occupa del trattamento dei dati personali, vengono perfettamente ad immedesimarsi in altrettanti concetti chiave con cui da qualche tempo a questa parte si viene sempre più a contatto: informativa e consenso.

Ormai qualunque sito web al giorno d'oggi, in basso oppure in un angolino della pagina, presenta un piccolo trafiletto, una piccola didascalia che fa riferimento nella maggior parte dei casi ai cosiddetti *cookies*, strumenti tecnologici che consentono di memorizzare dati riguardanti le sessioni di navigazione in Internet, come ad esempio preferenze, oppure realizzare meccanismi di autenticazione come possono esserlo i login: nell'istante in cui ognuno di noi legge quel particolare promemoria, probabilmente in un primo momento addirittura non notato, viene automaticamente informato della possibilità di utilizzo di quei dati (nel caso di specie, relativi alla navigazione sul web) per determinate finalità[10].

Questa situazione che viene a crearsi è proprio l'informativa, perciò il consenso non può che essere lo step successivo: il momento, l'*attimo fuggente* in cui con un clic (per rimanere nell'esempio informatico) ci si dichiara favorevoli e dunque consenzienti al trattamento di quei dati. Proprio lì, molto spesso su quel minuscolo pulsante della schermata.

Ovviamente quanto appena descritto non può che avere un mero scopo esemplificativo, però permette allo stesso tempo di sottolineare con quanta facilità, con i tempi che corrono, le informazioni personali possano essere utilizzate, in modo assolutamente legale, proprio per via dell'assolvimento da parte di coloro che intendono trattare i dati altrui, degli obblighi di informativa e consenso (come previsto in primis dal Codice della privacy e in secundis dal

---

[10] Obiettivo dei siti web che utilizzano i *cookies,* può essere magari migliorare la navigazione degli utenti rendendola più efficiente e rapida.

nuovo Regolamento UE). Senza che però rilevi che in questo caso informativa e consenso siano stati ottenuti con un semplice clic.

Quando infatti si fa riferimento a tali doveri, non necessariamente occorre riferirsi allo stereotipo del classico documento cartaceo sottoposto all'interessato il quale letteralmente prende consapevolezza del trattamento dei suoi dati e consente ciò attraverso l'apposizione fisica della sua firma.

Questo iter sicuramente può avvenire in casi di sottoscrizione di contratti od operazioni di una certa importanza per i quali risulti preferibile avere quella sicurezza, quella certezza che solo gli *scripta* possono conferire: nella realtà più comune, però, il procedimento di informativa e consenso è talmente semplificato che l'interessato può anche non accorgersene.

Innanzitutto perché vi può essere informativa anche oralmente, non soltanto per iscritto e in secondo luogo perché essa può "celarsi" in dei semplici cartelli, ad esempio affissi presso gli ingressi di locali commerciali o luoghi aperti al pubblico, indicanti magari la possibilità di una sorveglianza tramite videocamere: questo ultimo tipo di situazione è da qualificarsi a tutti gli effetti come informativa dal momento che indica le finalità del trattamento (motivi di sicurezza) e in alcuni casi anche l'identificazione del responsabile a cui rivolgersi per ulteriori informazioni e chiarimenti in merito.

Probabilmente, a questo punto, saranno già chiari i significati di informativa e di consenso: la prima non è altro che ovviamente una preventiva informazione nei confronti dell'interessato circa le finalità e le modalità del trattamento, la natura obbligatoria o facoltativa del conferimento di dati, le categorie di soggetti destinatari e gli estremi identificativi del titolare e/o del responsabile con eccezione della comunicazione di informazioni già in possesso del soggetto cui si riferiscono quei dati.

D'altro canto, affinché sia dunque possibile il trattamento dei dati personali da parte di privati oppure enti pubblici economici è necessario il consenso espresso liberamente dall'interessato, debitamente e precedentemente informato[11] nei modi richiamati poc'anzi, specificatamente in

---

[11] Si parla appunto di *consenso informato* il quale può richiedere anche un periodico aggiornamento dell'informativa e sovente un anche un periodico rinnovo del consenso a seconda delle specificità del trattamento.
PIZZETTI, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli. Pag. 219.

riferimento ad un trattamento chiaramente individuato, anche documentando il tutto per iscritto il che è sempre obbligatorio per quanto concerne dati sensibili[12].

Ovviamente esistono delle eccezioni, ossia casi in cui è possibile usufruire dei dati senza il consenso della controparte: ciò potrebbe accadere quando il trattamento è necessario per adempiere ad un obbligo previsto dalla legge o da fonte legislativa comunitaria, quando ci si trova dinnanzi all'esecuzione di obblighi derivanti da contratto, in casi di dati provenienti da pubblici registri, atti ed elenchi, in situazioni provenienti da attività commerciali altamente fidelizzate e infine per ragioni di sicurezza o di incolumità di terze parti[13]. E soprattutto, richiamando il caso dell'informativa che si esplicita tramite i cartelli di videosorveglianza nell'ambito di locali commerciali o aperti al pubblico, qui il consenso non è richiesto poiché risulterebbe troppo farraginoso richiederlo[14].

Tralasciando, a questo punto, per un momento ciò che avviene in contesti aziendali in riferimento alla sicurezza dei dati, alla difesa del patrimonio degli stessi anche attraverso tecnologie spesso informatiche ad hoc, cui sarà dedicato un apposito focus successivamente, anche attraverso un confronto con le novità del recente Regolamento, è necessario spendere qualche parola, qualche riga sulla autorità massima di controllo in tema di trattamento dei dati personali, ossia il Garante della privacy, formalmente noto come Garante per la protezione dei dati personali.

Il Garante nazionale

---

[12] I dati sensibili, dunque, vanno protetti in maniera più rigorosa infatti è previsto dal Codice che siano impiegati codici identificativi o tecniche di cifratura che rendano tali dati inintelligibili. Esempi concreti di dati sensibili possono essere informazioni circa lo stato di salute, la vita sessuale dell'individuo, persino la sua dieta alimentare poiché sono notizie potenzialmente idonee a rivelare la sfera più intima e riservata del soggetto.
SERRIELLO, A., 2016. *Quali dati personali sono considerati dati sensibili?* Unolegal Privacy Solutions [on-line], 7 settembre.
Disponibile su: http://www.unolegal.it/dati-personali-sono-dati-sensibili/ [data di accesso: 30/05/2017].

[13]CICCIA MESSINA, A., e BERNARDI, N., 2016. *Privacy e Regolamento europeo.* Milano: Wolters Kluwer Italia.

[14] Si pensi se prima di accedere a qualunque locale aperto al pubblico commerciale o meno, sia necessario ottenere il consenso di ciascun individuo; sarebbe letteralmente un caos, il sistema si ingolferebbe.

Esso, in base al Codice della privacy (precisamente all'articolo 153) che ha abrogato la legge 31 dicembre 1996 numero 675 che aveva istituito proprio tale figura, è da considerarsi come un'autorità amministrativa indipendente che si pone come obiettivo quello di assicurare la tutela dei diritti e delle libertà fondamentali, nonché il rispetto della dignità in caso di trattamento dei dati personali[15].

Il Garante è un organo collegiale costituito da quattro membri, eletti in egual numero da entrambi i rami del Parlamento, i quali in seguito provvedono alla nomina di un presidente di tale collegio: ovviamente la scelta dei potenziali membri da eleggere non è casuale, bensì risponde ad una esigenza di ricercare soggetti che irradino indipendenza di pensiero e che siano competenti nelle materie del diritto e dell'informatica.

Una figura istituzionale, certo, ma che sulla carta stando al Codice della privacy risponde ad un ampio ventaglio di funzioni e compiti: quasi lapalissiano il primo dovere del Garante, coerentemente con la sua denominazione, è quello di verificare e garantire per l'appunto che i trattamenti siano effettuati nel rispetto della disciplina in oggetto, anche riguardo la cessazione degli stessi.

Ciò può avvenire anche attraverso un'imposizione ai titolari del trattamento delle misure necessarie e consone affinché vi sia conformità con le disposizioni vigenti.

Questo sta a significare che in presenza, ad esempio, di reclami (a patto che siano non manifestamente infondati) il Garante ha la possibilità di disporre del blocco o del divieto di un trattamento illecito o non corretto qualora vi possa essere sentore di un concreto rischio di pregiudizio ad uno o più interessati. Indirettamente è possibile evincere un altro compito di questa autorità di controllo, cioè quello di esaminare i reclami e le segnalazioni degli interessati lesi in qualche modo, provvedendone su eventuali ricorsi.

Inoltre, davvero molto rilevante, è la tenuta dei registri relativi alle cosiddette notificazioni; un termine che certamente evoca un qualche tipo di adempimento da effettuare in favore del

---

[15] Emblematico può essere il caso della prima pronuncia del Garante nei confronti del social network Facebook; l'autorità di controllo italiana ricevendo l'istanza di un interessato, leso per via dell'utilizzo di terzi delle sue informazioni e dati personali al fine della creazione di un profilo falso, ha intimato allo stabilimento Facebook in Italia di procedere con la comunicazione dei dati all'interessato nonché con il blocco degli stessi.
MINAZZI, F., 2016. *Prima pronuncia del Garante contro Facebook.* Bruno e Ranieri Studio Legale Associato [on-line], 24 maggio.
Disponibile su: http://www.studiolegalebrunoeranieri.it/facebook-e-privacy-prima-pronuncia-del-garante-privacy-contro-facebook/news/225/2016/5/26 [data di accesso: 13/06/2017].

Garante dal momento che quest'ultimo opera come una sorta di organo a chiusura, a sigillo dell'intero sistema relativo al trattamento dei dati personali.

Adempimento ovviamente da parte del titolare, il quale è vincolato alla notificazione del trattamento cui intende procedere qualora esso riguardi dati genetici e biometrici indicanti l'ubicazione geografica dell'interessato, dati che afferiscano alla sfera sessuale e psichica oppure che rivelino lo stato di salute (quest'ultimo caso rappresenta una sorta di esenzione alla notificazione se ci si riferisce a medici di famiglia poiché la loro funzione richiede il naturale trattamento di dati riguardanti la salute dell'interessato); insomma la maggior parte dei dati personali.

Meglio così, si potrebbe ritenere, poiché vi è maggiore controllo sull'operato dei titolari da parte di un organismo super partes, che richiede anche delle comunicazioni aggiuntive obbligatorie qualora vi sia uno scambio di dati tra più titolari al contempo anche soggetti pubblici.

Cercando ora di evitare un asettico sproloquio enunciando il completo elenco dei compiti del Garante, situato lì inamovibile nel Codice perciò inutile riproporlo in questa sede, è necessario altresì rivolgere lo sguardo ad un particolare dovere, che rappresenta un raccordo al tema principale di questa trattazione: tale organo svolge anche la funzione di controllo o assistenza in materia di trattamento dei dati personali, prevista sopratutto da discipline comunitarie.

Una di queste legislazioni comunitarie cui si riferisce il Codice è il neo Regolamento dell'Unione Europea, 679/2016, proprio in tale materia: fondamentale, dunque, il ruolo del Garante che non solo funge da ponte tra la disciplina italiana vigente e la nuova fonte comunitaria, ma può anche essere considerato ai fini di questo elaborato un ideale punto di congiunzione tra i due temi.

Il nuovo orizzonte europeo

E' stato in precedenza affermato e più volte sottolineato che i tempi si evolvono, gli scenari cambiano e vi sono continui progressi soprattutto in campo scientifico-tecnologico perciò anche la materia della privacy deve necessariamente mutare pelle per potersi sempre difendere da eventuali nuove minacce.

Il Codice italiano sul trattamento dei dati personali discendeva a sua volta da una Direttiva comunitaria "madre" per così dire, la numero 46 del 1995: era quindi figlio di un' epoca in cui non era ancora avvenuta la celeberrima rivoluzione digitale, le persone si scambiavano

messaggi o corrispondenza tramite posta e francobolli, si informavano sulle ultime news leggendo i quotidiani e l'Internet non aveva ancora invaso le abitazioni di chiunque.

Per questo motivo anche le regolamentazioni, in questo caso sulla privacy, non prevedevano chissà quali grosse misure e provvedimenti poiché i pericoli erano da considerarsi ancora primitivi.

Ma con il mercato digitale e il world wide web, la situazione è cambiata così radicalmente e così rapidamente che persino la legislazione si è vista costretta a tenere il passo con l'innovazione: si è ritenuta indispensabile una sorta di aggiornamento delle normative per dare ordine al sempre più imponente flusso di dati che letteralmente corrono da un polo all'altro del globo con estrema semplicità.

Ciò è stato ottenuto dopo ventuno anni dalla famosa Direttiva 95/46/CE, passando per un iter legislativo durato quattro anni al termine dei quali è stato partorito il più volte citato Regolamento (UE) numero 679 del 27 aprile 2016[16], pubblicato in Gazzetta Ufficiale il 4 maggio successivo, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla loro libera circolazione nel territorio dell'Unione Europea.

Un passaggio da una direttiva ad un regolamento che sicuramente è funzionale a porsi ancor più a presidio della privacy dinnanzi alle minacce di recente affermazione, ma che al medesimo tempo fa riflettere sul motivo secondo cui il legislatore europeo abbia optato per la fonte-regolamento piuttosto che per la fonte-direttiva, impedendo così una naturale prosecuzione normativa.

Digredendo un attimo, un regolamento è direttamente applicabile e valevole erga omnes senza l'intermediazione statale, viceversa la direttiva entro un termine predeterminato necessita di un recepimento con legge interna da parte dello stato, il che può essere differente e disomogeneo tra uno stato membro e l'altro.

Ecco spiegata la scelta della fonte Regolamento: il legislatore comunitario per garantire maggiore omogeneità riguardo un tema così "caldo" ha preferito ricorrere a tale tipo di strumento.

Regolamento già vigente automaticamente, dunque, dal maggio scorso, ma applicabile soltanto a partire dal maggio 2018, una volta che siano decorsi due anni di *vacatio legis*

---

[16] Regolamento (UE) del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile. Disponibile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ITA [data di accesso: 16/05/2017].

quando dovrà verificarsi il perfetto allineamento tra la disciplina nazionale e quella regolamentaria.

Durante questo periodo di transizione le varie normative nazionali dovranno essere rese conformi al Regolamento, perciò risulta attualmente fondamentale per imprese e settore pubblico attrezzarsi per adeguare i trattamenti alle nuove linee guida, studiando ovviamente quali sono le novità e se vi sono eventuali similitudini, punti di contatto con la disciplina vigente, in questo caso, italiana.

Sostanzialmente per quanto riguarda le figure chiave cui compete il trattamento dei dati personali, ossia titolare e responsabile, non vi sono notevoli differenze con il Codice italiano: il primo in qualità di persona fisica o giuridica, autorità pubblica o altro organismo determina le modalità e le finalità del trattamento adottando adeguate misure tecnico-organizzative per dimostrare la conformità al Regolamento, e può ricorrere tramite contratto scritto ad un altro soggetto, il responsabile, che possa garantire la tutela dei diritti dell'interessato e il rispetto della disciplina comunitaria. Nulla di particolarmente nuovo rispetto al passato.

Dove si trova allora la novità, l'aggiornamento?

Esso risiede innanzitutto nella definizione del cosiddetto *rappresentante*, ossia quella persona fisica o giuridica stabilita nell'Unione Europea designata per iscritto a rappresentare un titolare o un responsabile straniero. Una sorta di mediatore per quanto riguarda una operazione di trattamento tra titolare e/o responsabile e soggetti interessati, cui si riferiscono i dati utilizzati dai primi, non appartenenti o non stabiliti nel medesimo Stato membro all'interno della UE. La nomina di tale rappresentante non è da applicarsi soltanto nei confronti di autorità pubbliche o in casi caratterizzati da un trattamento effettuato da un titolare straniero non in modo continuativo, bensì occasionale, oppure se esso riguarda particolari categorie di dati sensibili su scala ridotta.

In secondo luogo la figura di matrice italiana, per così dire, dell'incaricato al trattamento non viene affatto menzionata e quindi non disciplinata dal nuovo Regolamento; ciò, tuttavia, non impedisce di usufruire di soggetti assimilabili all'incaricato italiano, con le medesime funzioni, soprattutto in ambito di sicurezza dei dati. Al contempo, però, sorge il *responsabile alla protezione dei dati,* il "data protection officer" (argomento che verrà approfondito successivamente quando si discuterà specificatamente del contesto aziendale), figura di cui dovranno munirsi aziende pubbliche e private rispondenti a determinati requisiti.

Inoltre, tenendo ben a mente il compito di tenuta dei registri delle notificazioni in capo alla massima autorità di controllo italiana, il Garante, e quindi di contro l'obbligo da parte del

titolare di notificare la maggior parte dei trattamenti di dati personali, è necessario sottolineare che questo adempimento formale è stato de facto abolito dal Regolamento.

Il sostituto è un obbligo, in capo sia al titolare che al responsabile, di tenuta di appositi e rispettivi registri delle attività di trattamento. Il registro del primo deve indicare principalmente le sue generalità, le modalità e le finalità del trattamento come è consuetudine ormai, una descrizione generale delle misure tecnico-organizzative di sicurezza, i termini ultimi per l'eliminazione delle varie categorie di dati, i destinatari ed anche eventuali trasferimenti di dati verso paesi terzi.

Dall'altro lato il responsabile provvede a compilare il proprio registro indicando soprattutto le generalità del titolare del trattamento per il cui conto agisce e quindi ciascun trattamento effettuato in suo nome, conferendo le usuali garanzie di sicurezza a protezione dei dati da un punto di vista tecnico-organizzativo.

Avendo, dunque, cominciato a sbirciare nei meandri del Regolamento, è necessario a questo punto evidenziare come esso intenda all'interno delle cosiddette "disposizioni generali" segnare quello che è il suo perimetro di azione. Dapprima con una serie di definizioni, che un po' rappresentano il *passe-partout* per accedere alle diverse sezioni della disciplina, alcune di esse già presenti nel Codice e poc'anzi richiamate, altre invece del tutto innovative ed accennate qualche riga fa a mo' di antipasto. Sì, perché il 679/2016 non solo aggiunge categorie di figure quali il rappresentante e il data protection officer, bensì amplia fornendone una definizione più dettagliata il termine "dato personale" poiché si includono i significati di *dato genetico, biometrico* e *relativo alla salute,* non previsti dall'italiano d. lgs. 196/2003. I dati genetici sono quei dati personali che afferiscono alle caratteristiche genetiche ereditarie o acquisite di una persona fisica permettendo di ottenere informazioni sulla fisiologia della stessa; biometrici, invece, si intendono quei dati ottenuti da trattamenti tecnici molto sofisticati sulle particolarità fisiche, fisiologiche o comportamentali dell'individuo, quali possono esserlo l'immagine facciale o le impronte digitali, tali da identificarlo in modo univoco. Infine gli ultimi sono dati relativi ovviamente allo stato di salute fisica o psichica del soggetto in riferimento anche a prestazioni dei servizi sanitari nazionali.

In generale, inoltre, possono esserci diverse modalità di trattamento, aggiuntive rispetto alla definizione italiana classica in merito: sono introdotti i concetti di *profilazione* e di *pseudonimizzazione*[17]. Il primo riguarda qualsiasi forma di trattamento automatizzata

[17] CICCIA MESSINA, A., e BERNARDI, N., 2016. *Privacy e Regolamento europeo.* Milano: Wolters Kluwer Italia.

attraverso cui è possibile valutare situazioni relative a persone fisiche prevedendone aspetti come rendimento professionale, situazione economica o affidabilità.

Il secondo si riferisce ad un trattamento di dati personali tale per cui essi non siano più attribuibili ad uno e un interessato soltanto senza che vi siano informazioni aggiuntive: questo, per rendere più difficoltosa la violazione della privacy di quel soggetto attraverso una sorta di mescolamento di carte[18].

E proprio riguardo al trattamento dei dati personali, il Regolamento cerca di raggiungere due ben marcati obiettivi strettamente legati tra loro, ossia la tutela dei soggetti interessati e la circolazione dei dati di questi ultimi, a maggior ragione quando essi vengono scambiati o trasferiti: la presenza di molteplici livelli di protezione rappresenta un implicito vincolo, una limitazione alla libertà di circolazione che pure è un principio cardine su cui si basa la stessa UE. Va ricercato un equilibrio tra chi è meritevole di tutela e chi tratta i dati sia in modo automatizzato sia manualmente[19]. Ovviamente esistono anche qui delle eccezioni: la disciplina non trova terreno fertile per quanto concerne trattamenti effettuati da persone fisiche non già nell'ambito di attività commerciali o professionali, oppure per ragioni legate alla politica estera, alla sicurezza o alla giustizia oppure in caso di discipline che esulino dall'area di competenza dell'Unione. Chiaramente il 679/2016 si muove entro i confini europei, proprio perché si è cercato di rendere omogenea la legislazione almeno in ambito comunitario: se si va oltre, la situazione cambia anche con riferimento al tema della privacy e dei dati personali. Il Regolamento si applica comunque in primo luogo qualora il soggetto che tratti i dati sia stabilito nell'Unione, anche se il trattamento nella sostanza sfocia al di fuori e in secondo luogo se il soggetto interessato risulti in qualche modo collegato con il territorio europeo, ad esempio avendovi domicilio.

Una disciplina così composita non può anche che prevedere dei principi che in qualche modo dovrebbe guidare l'operato di coloro che hanno a che fare con dati personali altrui: tali principi sono sostanzialmente allineati con quelli previsti e già discussi per quanto riguarda il Codice italiano. Ovviamente su tutti spicca il presupposto di liceità che dipende direttamente dal consenso al trattamento per una o più finalità: l'onere probatorio grava sulle spalle del

---

[18] La pseudonimizzazione si differenzia dai dati anonimi, i cosiddetti big data, poiché nel primo caso si parla di codici abbinati a ciascun individuo il quale può essere intercettato con l'utilizzo di altre informazioni.

[19] Nel caso di un trattamento di dati in modo manuale, essi devono essere conservati in appositi archivi.

titolare il quale deve dimostrare che l'interessato sia consenziente verbalmente o per iscritto, anche con mezzi elettronici, salva la possibilità di revocare il consenso in qualsiasi momento, il che non pregiudica la liceità del trattamento sino ad allora.

Eccezioni a questa fattispecie possono riguardare situazioni di contratti tra le parti oppure casi di perseguimento di un interesse legittimo da parte del titolare. Nel primo caso la necessità di esecuzione del contratto o di obblighi precontrattuali può prescindere da una forma di consenso troppo vincolante.

D'altra parte i legittimi interessi del titolare, come la prevenzione di frodi, possono comunque rendere lecito il trattamento eludendo così il consenso; a patto che non prevalgano diritti o libertà fondamentali dell'interessato, specie se minore.

Dopodiché il Regolamento espone in maniera molto dettagliata i principi di limitazione delle finalità e di minimizzazione dei dati: essi, certamente esatti o perlomeno aggiornabili, debbono essere adeguati, pertinenti rispetto agli scopi originari e non oltre conservati comunque in modo integro e riservato. Ovviamente sono disciplinati anche i più importanti principi di correttezza e trasparenza: di pari passo con l'attuale normativa italiana vigente deve essere sottolineato e previsto il rispetto delle esigenze reciproche tra le parti assicurandosi che l'interessato sia totalmente consapevole di ciò che sta accadendo o che accadrà ai suoi dati.

E la trasparenza[20] può sorgere solo se le informazioni circa il trattamento sono per l'interessato facilmente comprensibili, snelle e sintetiche, ricorrendo a linguaggi chiari, sovente accompagnati da immagini o visualizzazioni il che è molto frequente su Internet.

Quasi fotocopiando il d. lgs. 196/03, sono anche a livello comunitario previsti molteplici diritti che rappresentano una sorta di scudo per l'interessato, a partire da quelli di accesso e rettifica già affronti in precedenza fino ad arrivare ad una definizione di informativa molto dettagliata e completa.

L'interessato deve essere informato che vi è un trattamento che lo riguarda, con tutte le forme di tutela del caso, sia quando i dati vengano raccolti presso lo stesso sia quando invece siano

---

[20] Il concetto di trasparenza non è meramente ideologico e teorico, anzi tale principio viene equiparato ai più volte richiamati principi di liceità e correttezza dal momento che il testo originale del Regolamento stabilisce che i dati devono essere trattati *lawfully, fairly and in a trasparent manner*, quindi lecitamente, lealmente ed in modo trasparente.
PIZZETTI, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli.
Cfr. Regolamento del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile.Art.5.

collezionati presso soggetti terzi. Nella prima fattispecie il titolare deve debitamente assolvere al dovere di informativa nell'istante in cui i dati sono ottenuti, riportando nozioni e informazioni sostanzialmente non dissimili da quelle previste dal Codice italiano: nel caso in cui il titolare necessitasse ulteriormente dei dati per finalità eccedenti rispetto a quelle originarie deve fornire le informazioni aggiuntive conseguenti.

Viceversa se si considera una situazione ove i dati non siano raccolti direttamente presso l'interessato, quest'ultimo ha il diritto di essere informato dal responsabile entro un termine di tempo ragionevole, al massimo di un mese, dal conseguimento dei dati oppure al momento della prima divulgazione qualora i dati vengano comunicati ad altri destinatari. Similmente al caso di raccolta diretta dall'interessato, si prevedono le medesime modalità in caso di trattamenti eccedenti. Certamente l'informativa si disapplica non solo quando le informazioni sono già possedute dalla controparte, ma anche qualora la comunicazione delle stesse risulti impossibile o comporti sforzi sproporzionati da parte di chi ne ha l'onere.

Vere e proprie novità, invece, possono essere considerati il *diritto all'oblio,* la *portabilità dei dati*[21]*,* e la materia della *profilazione on-line.* Certamente il primo non è da associarsi al fiume Lete che secondo la mitologia greca e romana conduceva all'Oltretomba, bensì è da considerarsi come il diritto di un individuo ad essere dimenticato, a non essere più ricordato per delle vicende che lo riguardavano in passato: una sorta di *damnatio memoriae* successiva ad un arco temporale più o meno ristretto, ma comunque circoscritto, utile ad informare la collettività riguardo quelle vicende. Questa definizione, a dire il vero molto filosofeggiante, traslata nella disciplina regolamentaria attesta il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo in presenza di determinate condizioni: tra le altre, quando i dati non sono più necessari rispetto alle finalità per cui sono stati raccolti, quando essi sono trattati illecitamente, se

---

[21] SCAFATI, G., e STUDIO LEGALE STELE' PERELLI, 2016. *La "privacy europea", il Regolamento UE 679/2016.* Il Sole 24ore [on-line], 16 maggio. Disponibile su: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php [data di accesso: 14/04/2017].

debbono essere cancellati dinnanzi ad obblighi legali oppure nel caso in cui venga revocato il consenso[22].

Per quanto concerne la portabilità dei dati[23], si tratta del diritto a ricevere in formato strutturato ed unico i dati personali forniti ad un titolare, in modo che essi possano essere trasmessi a cura dell'interessato senza impedimenti ad un altro titolare, magari fornitore di un differente servizio.

La materia, invece, della profilazione on-line risulta alquanto più complessa: è stato in precedenza affermato che si intende quel trattamento automatizzato volto ad analizzare e/o prevedere aspetti relativi alla persona fisica dell'interessato in questione. Generalmente egli ha il diritto di non essere sottoposto a delle decisioni basate esclusivamente su un'operazione meccanica, computerizzata tranne casi di previsioni normative finalizzate a scongiurare frodi o evasioni fiscali ad esempio; comunque l'interessato ha sempre diritto a ricevere puntuali informazioni riguardanti le modalità di profilazione[24] e ad opporsi ad essa fatta salva la possibilità dell'Unione o degli stati membri di imporre limitazioni a presidio di interessi superiori, quali la pubblica sicurezza. Qualora sia consentita la profilazione, orbene, risulta necessario ricorrere a procedure matematico-statistiche appropriate, prevedendo una eventuale

---

[22] Un caso pratico in questo senso può essere quello tratteggiato nel provvedimento del 24/11/16 ad opera del Garante; nella sostanza è un ricorso da parte di un imprenditore in quanto si sentiva leso poiché sul motore di ricerca in Internet risultavano dei link in cui il suo nome era associato a dei reati.
Perciò il soggetto in questione invocava il diritto all'oblio e quindi alla cancellazione di tali informazioni che in qualche modo, veritiero o falso, riconducevano a lui.
FAMILIARI, S., 2017. *Un caso pratico di diritto all'oblio: la ricerca assistita di Google.* Il Quotidiano Giuridico [on-line], 6 marzo.
Disponibile su: http://www.quotidianogiuridico.it/documents/2017/03/06/un-caso-pratico-del-diritto-all-oblio-la-ricerca-assistita-di-google [data di accesso: 13/06/2017].

[23] Portabilità significa già tutto quello che è ben noto grazie all'esperienza, per esempio, dei contratti con le compagnie telefoniche nella circostanza in cui si cambia gestore telefonico tenendo invariato il numero senza che l'interessato provveda materialmente a comunicare il numero stesso al nuovo gestore. Anche in questo caso, il titolare rifiutato deve trasmettere i dati al "collega" scelto.
MARINI, P., 2016. *Oblio e portabilità dei dati: novità dal nuovo Regolamento Privacy europeo.* Il Quotidiano Giuridico [on-line], 26 luglio.
Disponibile su: http://www.quotidianogiuridico.it/documents/2016/07/26/oblio-e-portabilita-dei-dati-novita-dal-nuovo-regolamento-privacy-europeo [data di accesso: 13/06/2017].

[24] In ambito commerciale la profilazione degli utenti è uno strumento del cosiddetto marketing mirato, che fa largo uso di questa tecnica per ottenere accurate analisi riguardo potenziali clienti, al limite della legalità.

rettifica delle variabili e in aggiunta cercando di minimizzare la possibilità di errori che producano inesattezze dei dati, i quali sono sempre meritevoli di tutela. Mai, però, la profilazione può avere ad oggetto un minore.

A questo punto, perciò, risulta necessario aprire una piccola parentesi avente come protagonisti i minori, cui sono dedicate sia dal Codice che dal nuovo Regolamento apposite e aggiuntive misure di sicurezza e tutela dal momento che essi possono essere meno consapevoli dei rischi che corrono relativamente ad una anomala diffusione dei loro dati.

Innanzitutto il trattamento dei dati personali dei minori aventi età inferiore ai 16 anni, o compatibilmente con norme nazionali che possono abbassare tale soglia sino ai 13 anni, risulta lecito solo se il consenso sia stato espresso dal titolare della responsabilità genitoriale. Questa specifica protezione riguarda, soprattutto in questi tempi recenti, l'utilizzo di dati personali dei minori al fine di creazione di profili di personalità relativi ai social networks: in questi casi qualsiasi informazione o comunicazione concernente un eventuale trattamento deve essere fornita con un linguaggio semplice ed accessibile. Chiaramente il titolare è tenuto ad adoperarsi nei limiti della ragionevolezza a verificare o che il minore abbia almeno 16 anni o che vi sia stato consenso di coloro che ne detengano la responsabilità genitoriale.

Chiusa questa breve sebbene doverosa parentesi, è ovviamente del tutto normale ritenere che il Regolamento debba essere sorvegliato e garantito per quanto attiene alla sua applicazione da una autorità di controllo espressamente prevista: figura che in Italia è incorporata nel più volte nominato Garante della privacy.

Stando al 679/16, ogni stato membro nell'Unione deve munirsi di uno o più organismi di controllo assolutamente autonomi e indipendenti secondo le medesime modalità incluse nel d. lgs. 196/03. La nuova disciplina comunitaria assegna alle varie autorità di controllo nazionali un pacchetto costituito da tre categorie di poteri. I *poteri di indagine* permettono soprattutto di notificare al titolare e/o al responsabile presunte violazioni del Regolamento e quindi ottenere dagli stessi accesso a tutti i dati personali trattati, dopodiché consentono di condurre letteralmente indagini sotto forma di attività di revisione sulla protezione dei dati ed infine di ingiungere di fornire ogni informazione di cui l'autorità necessiti. Secondariamente, attraverso i *poteri correttivi* è possibile avvertire ed ammonire i soggetti che trattano i dati riguardo una possibile violazione delle norme, perciò di conseguenza prescrivere la conformità alla disciplina ed infine imporre limitazioni più o meno provvisorie al trattamento attraverso rettifiche o cancellazione di dati in aggiunta spesso a sanzioni amministrative pecuniarie. Da ultimi, non per importanza, disponendo dei *poteri autorizzativi e consultivi*

l'autorità di controllo fornisce consulenza al titolare mediante pareri su progetti di codici di condotta oppure rilasciando certificazioni. E proprio riguardo a questi ultimi due temi, una rilevante novità del Regolamento consiste nell'istituzione di strumenti di certificazione e sigilli, nonché marchi di protezione dei dati[25] che consentono agli interessati di verificare ex ante in modo ancor più trasparente il livello di tutela degli stessi.

L'adozione dei codici di condotta è assolutamente volontaria, anche se ovviamente altamente incoraggiata dalle autorità di controllo, avente lo scopo di dimostrare la conformità alle disposizioni per quanto concerne i rischi connessi al trattamento dei dati; ne deriva che il limite fisiologico di tali codici consista nella loro auto-referenzialità, cioè nella circostanza che è l'impresa stessa a dettare e quindi approvare suddetti codici affermandone il rispetto.

Al contrario la certificazione, proveniente anche qui autonomamente dal titolare, deve essere sottoposta al vaglio degli organismi di controllo competenti che devono approvarla anche in caso di rinnovi successivamente al triennio di durata standard, qualora rimangano rispettati i consueti criteri di allineamento rispetto alla disciplina comunitaria[26].

Fondamentale, inoltre, il ruolo della autorità garante anche in casi di cosiddetta *one stop shop*: quando accade che il titolare o il responsabile siano stabiliti in più stati membri oppure quando il trattamento possa verosimilmente riferirsi a soggetti interessati appartenenti a più nazioni dell'Unione, l'autorità dello stabilimento principale del titolare o del responsabile funge da capofila rispetto alle altre comunque cooperando coerentemente con gli altri garanti anche riguardo la presa di decisioni vincolanti.

Gerarchicamente al di sopra degli organismi di controllo nazionali, si trova il Comitato Europeo per la protezione dei dati personali ossia una autorità indipendente dalla UE munita di personalità giuridica e composta dalle figure di vertice di un'autorità di controllo per

---

[25] Si faccia caso che al giorno d'oggi tutti i maggiori siti web in Internet presentano come protocollo di comunicazione e trasferimento di dati la dicitura iniziale *https* piuttosto che il vecchio *http*: questa aggiunta sta ad indicare proprio un marchio di protezione di dati che garantisce maggiore sicurezza agli stessi.

[26] Quindi i codici di condotta nascono come strumenti di autodisciplina elaborati dalle singole imprese affinché siano sanciti principi di orientamento delle attività o norme tecnico-procedurali, mentre le certificazioni sono dettate da un ente di normazione, quale può essere il Garante, terzo ed indipendente.
MARINI, P., 2017. *Regolamento europeo Privacy: i codici di condotta e le certificazioni.* Il Quotidiano Giuridico [on-line], 27 febbraio.
Disponibile su: http://www.quotidianogiuridico.it/documents/2017/02/27/regolamento-europeo-privacy-i-codici-di-condotta-e-le-certificazioni [data di accesso: 13/06/2017].

ciascuno Stato, avente il compito di favorire l'applicazione del Regolamento. Una sorta di garante dei garanti, un garante europeo che cerca di omogeneizzare le varie interpretazioni nazionali sulle disposizioni comunitarie.

Soprattutto quando occorre bilanciare il rapporto tra protezione dei dati personali e diritto alla libertà di espressione, di informazione e ancora più crucialmente quando si parla di relazione tra cittadino e pubblica amministrazione; in questi ambiti, tuttavia, il 679/16 fa esplicito rinvio alle discipline nazionali. Una lacuna del Regolamento oppure una precisa intenzione del legislatore europeo? Quello che è certo è che tali discipline territoriali dovrebbero cercare di favorire un equilibrio tra il principio di pubblico accesso, e quindi riutilizzo, ai documenti ufficiali con l'interesse relativo alla protezione dei dati personali; un'equazione che molto spesso non è granché rispettata.

Perciò se da un lato Comitato Europeo per la protezione dei dati e autorità di controllo nazionali possono fungere come una tutela discendente dall'alto, top-down, dall'altro sono state pensate dalla nuova disciplina due forme di tutela provenienti direttamente dagli interessati, bottom-up: la possibilità di un ricorso amministrativo se non addirittura giurisdizionale. L'interessato, persona fisica o giuridica che sia, che si senta leso nei suoi diritti in riferimento ad una presunta violazione della privacy può proporre un ricorso giurisdizionale effettivo dinnanzi alle autorità giurisdizionali competenti dello stato membro ove siano stabiliti titolare e responsabile del trattamento, promuovendo inoltre reclamo alla autorità garante corrispondente. Quindi, il Regolamento prevede che qualunque interessato che subisca un pregiudizio materiale o immateriale causato da un disallineamento rispetto alle disposizioni vigenti, ha il diritto di ottenere un risarcimento da parte del titolare o del responsabile, il quale ultimo risponde solo qualora non avesse adempiuto agli obblighi normativi specificatamente a lui rivolti oppure alle istruzioni impartite dal primo. Tali figure sono, invece, esonerate dalla responsabilità e quindi anche dal risarcimento se, ribaltandone l'onere probatorio, dimostrino che l'accadimento dannoso non risulta in alcun modo a loro imputabile.

In possesso, a questo punto, degli strumenti principali e necessari per affrontare il Regolamento, si passi ora ad osservare e studiare come nella sostanza le recenti disposizioni siano calate nella realtà di chi tratta quotidianamente dati personali non propri, tenuto a fare ciò nel rispetto di prevenzioni e misure di sicurezza volte ad arginare il seppur minimo pregiudizio nei confronti di tali dati.

Capitolo 3

Cosa cambia in ambito aziendale?

Sino a questo momento la trattazione ha assunto un tono molto spesso troppo teorico, a tratti somigliante ad un mero elenco di regole, obblighi e doveri; è dunque giunto il tempo di scalfire l'ideale parete costituita da pagine, articoli e commi e di calarsi nella realtà concreta aziendale.

Più volte in precedenza l'attenzione si è soffermata sul fatto che l'intera legislazione italiana vigente da una parte e quella comunitaria neonata dall'altra riguardino un trattamento di dati personali non a scopo, si perdoni l'infelice gioco di parole, personale bensì economico, aziendale oppure per finalità di stampo pubblico.

Ciò sta a significare che sono tenuti all'applicazione e al rispetto delle varie procedure e dei vari doveri, di cui al precedente capitolo, non ad esempio i due ragazzi che conosciutisi per la prima volta decidono di scambiarsi i numeri di cellulare, ma al contrario magari società commerciali, nel momento in cui qualche cliente conferisce i propri dati affinché ottenga un qualche tipo di beneficio come molto banalmente il rilascio di una fidelity card.

Sarà, quindi, facilmente comprensibile quanto il tema del trattamento risulti legato a doppio filo con il contesto aziendale a prescindere dal fatto che si tratti di pubblico piuttosto che privato oppure economico. Una precisazione, però, è meritevole di effettuazione: ovviamente i dati e le informazioni che possono essere trattati non riguardano in modo esclusivo soggetti esterni ad una particolare realtà aziendale come clienti commerciali o utenti di una pubblica amministrazione desiderosi di un particolare prodotto o della fruizione di un determinato servizio. Occorre allargare gli orizzonti includendo nella tutela anche gli interessi alla riservatezza dei soggetti che vivono, per così dire, all'interno del perimetro aziendale: i lavoratori stessi.

A mo' di esempio: la società *tal dei tali* certamente tratta i dati personali dei suoi clienti per determinate finalità quali possono essere di marketing, economiche, di ricerca…, ma allo stesso tempo quasi inconsciamente abbraccia anche le informazioni dei propri lavoratori. Si potrebbe pensare che sia una faccenda del tutto ovvia, scontata, però contemporaneamente non bisogna sottovalutare questo argomento. L'impresa titolare di un qualche tipo di trattamento, si prenda il caso più banale del trattamento dei dati personali dei clienti, risulta contemporaneamente datrice di lavoro di un numero più o meno esteso di lavoratori perciò necessariamente detiene i dati e le informazioni più rilevanti che occorrono affinché si instauri

legalmente un rapporto lavorativo, nella maggior parte dei casi attraverso curricula vitae. Bene, questo è a tutti gli effetti un trattamento poiché si parla di una operazione innanzitutto di raccolta e in seguito di conservazione.

Particolare pericolo, però, relativamente alla privacy, alla riservatezza di questa particolare categoria di soggetti deriva dalla questione del controllo sui lavoratori durante l'attività lavorativa.

Ovviamente non è certo questa la sede per dibattere riguardo la ragione o meno da parte del datore di lavoro ossia l'impresa di controllare il lavoratore, poiché si sfocerebbe in contesti giuslavoristici, ma è innegabile che, qualora si ammetta il controllo, una naturale conseguenza sarebbe la più o meno ampia compressione del diritto alla privatezza del lavoratore. Perciò è necessario affrontare questa breve digressione.

Lo Statuto dei lavoratori

Tale disciplina è contenuta nella legge numero 300 risalente al 1970, il cosiddetto Statuto dei lavoratori che sostanzialmente pone un limite di fonte legale al potere del datore di lavoro. A garanzia della privacy del lavoratore, infatti, il datore non può in modo assoluto finanche al momento dell'assunzione indagare sulle opinioni politiche, religiose o sindacali oppure su qualunque tipo di informazione che non sia strettamente necessaria ai fini della valutazione dell'attitudine professionale del lavoratore[27]; il datore, quindi, non può minimamente avvicinarsi a tali dati sensibili e di conseguenza neanche trattarli. Troppo semplice se solo fosse questo l'unico "problema"; le innovazioni tecnologiche e la progressiva informatizzazione delle organizzazioni aziendali hanno dato alla luce nuove problematiche relative alla privacy degli individui in ambito lavorativo. Il progresso tecnico ha consentito ai datori di lavoro di aumentare l'efficienza produttiva attraverso una sempre più estesa ed intensa sorveglianza, tramite videocamere e circuiti chiusi, anche delle prestazioni dei lavoratori. E non solo: moderni sistemi elettronici come *log*, *cache memory*, *bookmarks*[28] permettono il controllo della attività lavorativa svolta, gli accessi informatici e i siti Internet visitati.

---

[27] L. 20 maggio 1970, n°300, art.8.

[28] Il primo permette la registrazione, il riconoscimento o l'accesso a particolari piattaforme informatiche, il secondo consente la memorizzazione di dati più volte utilizzati per garantirne un successivo veloce riutilizzo, il terzo è un segnalibro che rappresenta una scorciatoia per arrivare agli indirizzi delle pagine web.

Invasività brutale ed esplicita nel primo caso, decisamente subdola e silente nel secondo. A questo punto qualcuno potrebbe lecitamente domandarsi se la videocamera "sparata" sulla testa del lavoratore o la situazione in cui il datore osserva quante volte Tizio dalla sua postazione d'ufficio abbia letto on-line un quotidiano sportivo siano possibilità che possono accadere del tutto legalmente. Tecnicamente no: la normativa attualmente in vigore dello Statuto[29] asserisce che qualunque tipo di strumento o impianto audiovisivo da cui scaturisca anche la possibilità di controllo a distanza dell'attività del lavoratore può essere impiegato solo e soltanto per ragioni di sicurezza, per esigenze organizzativo-produttive e a tutela del patrimonio aziendale previo accordo collettivo stipulato con le rappresentanze sindacali oppure in mancanza con l'Ispettorato del lavoro. Eccezion fatta per i casi in cui tali strumenti siano utilizzati dal lavoratore per rendere la propria prestazione o se si tratta di strumenti di registrazione di accessi e presenze: per queste situazioni non è necessario il rispetto di tutta la trafila descritta in precedenza. In parole povere, vi è assolutamente divieto per il datore di lavoro di ricorrere a mezzi di mero controllo, quindi inutili al lavoratore per adempiere ai propri doveri; nei casi restanti e dunque in presenza delle esigenze sopra citate il datore può installare, ad esempio, videocamere di sorveglianza coinvolgendo nella decisione organi sindacali o statali predeterminati nel caso in cui il controllo abbracci indirettamente anche i lavoratori. Sfortunatamente la disciplina vigente in tema di trattamento di dati personali, ossia il Codice della privacy, non contiene una regolamentazione specifica riguardante i rapporti di lavoro, perciò senza dilungarsi troppo sul tema è opportuno ricondurre anche queste situazioni di "invasione" sotto il più ampio cappello della tutela dei dati personali e della privacy in senso generale.

La sicurezza dei dati

Tale difesa (in senso *tout-court,* da ora in poi senza distinzioni tra dati di lavoratori e di altri soggetti), dunque, non si circoscrive nell'ambito di una postulazione di comportamenti corretti ad opera dei soggetti che trattano i dati in funzione dei supremi principi di liceità e correttezza, bensì si estende imponendo dei sistemi che concretamente garantiscono la protezione della sfera privata dell'interessato[30]. Al giorno d'oggi, infatti, per le aziende e le

---

[29] L. 20 maggio 1970, n° 300, art.4.

[30] SITZIA, A., 2013. *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali.* Padova: Cedam. Pag. 129.

imprese i dati rappresentano un asset fondamentale per il loro successo sul mercato; nessuna di esse desidererebbe mai che le liste dei propri clienti, i dati dei propri impiegati o dirigenti e talvolta i segreti industriali finissero nelle mani della concorrenza o di qualche malfattore. Secondo il Codice, perciò, i dati oggetto di trattamento debbono essere custoditi e controllati mediante l'adozione di misure idonee di sicurezza che prevengano eventuali rischi di distruzione o perdita, anche accidentale, e di accessi o trattamenti non autorizzati. In un orizzonte più ampio, fatto salvo quanto detto poc'anzi, i titolari sono comunque tenuti ad adottare misure di sicurezza minime individuate dalla stessa fonte legislativa[31]. Misure *idonee* da una parte e *minime* dall'altra; concetti differenti seppur complementari.

Il concetto di *idoneità* delle misure omonime è di per sé variabile poiché da rapportare alle conoscenze acquisite in relazione al progresso tecnico, alla natura dei dati e alla specificità di questo o quel trattamento e quindi aggiuntivo rispetto alle misure minime di genesi legale. L'omessa adozione rilevata in seguito ad una violazione di dati può causare in capo a titolare e responsabile un'azione risarcitoria in sede civile evitabile soltanto con la dimostrazione, capovolto l'onere probatorio, di aver impiegato tutte le opportune misure. Per rendere tracciabili alcune operazioni fiscali o bancarie può essere previsto, come misura idonea, l'obbligo di adottare specifici sistemi di monitoraggio con alert automatici che segnalino intrusioni, accessi e comportamenti anomali.

Per quanto attiene alle misure *minime*, invece, esse sono espressamente provenienti dal legislatore stesso. In caso di trattamenti mediante l'ausilio di strumenti elettronici devono essere previste procedure di gestione delle credenziali di autenticazione (password…), quindi di volta in volta verifica e convalida di chi accede al sistema, dopodiché appositi sistemi di autorizzazione che consentano solo specifiche attività predefinite; evidenziando anche l'utilizzo di antivirus o altri tipi di protezione informatica sempre aggiornati oppure di tecniche di crittografia volte a fornire maggiore tutela ai dati più sensibili. Inoltre occorre essere preparati a gestire situazioni di crisi attraverso la predisposizione di copie di backup che preservino i dati e ne garantiscano una fruizione futura.

La "nuova" sicurezza dei dati

Idea "italiana" di sicurezza sostanzialmente confermata con la neonata disciplina comunitaria sebbene con qualche correttivo.

---

[31] Dlgs. 30 giugno 2003, n°196, artt. 31 e 33.

Il Regolamento, infatti, prevede misure di sicurezza idonee da adottare sulla base di una valutazione dei rischi e una valutazione d'impatto, anche nota come *data protection assessment.* Ovviamente non risultano esplicitate nel nuovo testo normativo tramite elenco le varie misure cosiddette idonee, le quali semplicemente possono essere tecniche od organizzative e devono essere parametrate in funzione dei costi di attuazione delle stesse, dell'oggetto, della natura e della finalità del trattamento e della gravità di rischio per le libertà e diritti delle persone fisiche; questo ultimo aspetto sfocia appunto in quella che è la valutazione dei rischi, sempre necessaria come è sempre necessaria la sicurezza dei trattamenti[32].

La valutazione d'impatto, viceversa, nella sostanza sostituisce l'obbligo generale di notificazione del trattamento all'autorità di controllo, la quale comunque deve redigere un elenco delle varie tipologie di trattamento sottoposte a questo dovere. Questo tipo di valutazione si rivela essenziale in caso di trattamenti su larga scala caratterizzati da una notevole quantità di dati personali.

Il *data protection assessment* deve descrivere tali trattamenti sistematici e le loro finalità; in seguito deve stimare le necessità e la proporzionalità dei trattamenti in funzione delle finalità ed infine deve contenere le misure previste per affrontare eventuali rischi garantendo così la sicurezza dei dati degli interessati. Nella peggiore delle ipotesi, qualora emerga da tale valutazione che il rischio non possa essere ragionevolmente attenuato mediante l'uso della tecnologia oppure per via degli elevati costi di attuazione risulta necessario consultare preventivamente l'autorità di controllo, ossia il Garante, che pronunciandosi entro un tempo predeterminato si riserva anche di intervenire con il blocco dei trattamenti o con misure interdittive.

Se tutte queste barriere innalzate per prevenire violazioni dei dati personali dovessero cedere, si parlerebbe allora di *data breach*.

---

[32] CICCIA MESSINA, A., e BERNARDI, N., 2016. *Privacy e* Regolamento *europeo.* Milano: Wolters Kluver Italia. Pag. 53.

Non appena viene a conoscenza di una avvenuta violazione, il titolare deve notificare all'autorità di controllo di turno[33] senza ingiustificato ritardo, se possibile entro 72 ore[34], la natura della violazione con un calcolo approssimativo riguardante il numero degli interessati lesi in questione, le probabili conseguenze e le misure già adottate o adottabili di lì a poco. E' comunque plausibile che in casi di violazioni dei dati personali i soggetti lesi, poiché tali dati sono a loro riferibili, non vengano debitamente avvisati? Certamente non è così; il titolare del trattamento deve comunicare anche all'interessato senza indebito ritardo in caso di rischio elevato per i diritti e le libertà individuali in modo di consentirgli di assumere tutte le precauzioni necessarie.

Comunicazione non necessaria qualora invece richieda sforzi eccessivamente sproporzionati oppure quando il titolare abbia già messo in atto preventivamente tutte le misure tecnico-organizzative idonee alla protezione o anche successivamente in modo da scongiurare ulteriori rischi.

Le principali novità "aziendali" del Regolamento: *privacy by design, privacy by default,* principio di *accountability*

Proseguendo lungo la direttrice relativa alla sicurezza dei dati e alla protezione degli stessi, avendo discusso riguardo l'analisi dei rischi con annessa modalità di perpetrazione degli stessi, risulta adesso necessario evidenziare come la gestione del rischio in primis e la eventuale violazione dei dati personali in secondo luogo non debbano essere inquadrate come attività estemporanee, a sé stanti rispetto al trattamento o marginali poiché inerenti casi limite.

---

[33] Nel caso italiano, il Garante per la protezione dei dati personali.

[34] PANETTA, R., 2013. *Data breach: nuovo provvedimento del Garante Privacy sulle modalità di notifica.* Il Sole24ore [on-line], 10 maggio.
Disponibile su: http://www.diritto24.ilsole24ore.com/avvocatoAffari/mercatiImpresa/2013/05/data-breach-nuovo-provvedimento-del-garante-privacy-sulle-modalita-di-notifica.php [data di accesso: 30/05/2017].

Anzi in base al nuovo Regolamento nell'ambito della tutela dei dati vengono introdotti i neonati concetti di *privacy by design*[35] e *privacy by default.*

Nel primo caso si richiede la predisposizione di un piano, di una progettazione (traduzione di "design"), per l'appunto, nel cui contesto dovranno essere individuate e muoversi appropriate misure tecnico-organizzative proporzionate alla minaccia in modo da garantire una risposta efficace e tempestiva. Da un punto di vista logico, mediante un approccio alla protezione dei dati sin dalla progettazione non si adottano misure di sicurezza a posteriori, bensì ex ante in funzione delle varie ipotesi di trattamento. Un esempio in questo senso potrebbe essere la creazione di software antivirus che nell'atto di scansione delle pagine web visitate inevitabilmente trattano dei dati di navigazione, ma contemporaneamente sono programmati per eliminarli dopo un certo periodo di tempo in modo da ridurre al minimo potenziali rischi di violazione della privacy.

Viceversa in tema di privacy by default occorre far riferimento a tutte quelle situazioni per le quali vale la regola "Se nulla faccio, nessun mio dato deve essere acquisito"[36]. Generalizzando, l'interpretazione secondo un approccio alla protezione dei dati per impostazioni predefinite in base al Regolamento sta a significare che è proibita la raccolta, la misurazione o la condivisione di un qualunque dato personale senza che vi sia stato un esplicito consenso da parte dell'interessato; si sottolinei ancora una volta come il silenzio e l'inattività non possano mai costituire una forma tacita di consenso.

Le applicazioni di questo tipo di approccio sono diverse: molto banalmente un servizio di social networking deve adottare tutte quelle misure affinché le informazioni di determinati soggetti siano visibili pubblicamente solo se essi una volta collegatisi al sito danno specifica autorizzazione. Oppure un responsabile di un trattamento che voglia impostare un sito web deve porre particolare attenzione ad apportare tutte le regolazioni o i modelli operativi per i

---

[35] Questo concetto è stato inizialmente promosso dalla Commissaria dell'autorità di controllo canadese della provincia dell'Ontario, Ann Cavoukian, la quale nel 2009 pubblicò uno specifico documento intitolato "*Privacy by design, the 7 fundamental principals"*. Già in precedenza, però, il tema era stato ampiamente discusso ed esaminato nel 2007 durante il Congresso internazionale delle autorità garanti. Dopodiché, ad oggi, è entrato a far parte del sistema europeo sulla protezione dei dati personali.
PIZZETTI, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli. Pag. 287.

[36]BIAISOTTI, A., 2016. *Il nuovo regolamento europeo sulla protezione dei dati.* Roma: EPC editore. Pag.546.

quali vige il principio che nessun dato può essere acquisito senza un preventivo consenso dell'interessato.

Certamente questo tipo di approccio, invero molto frequente in Internet, comporta la comparsa di numerosi messaggi di avvertimento e di allerta richiedenti di volta in volta il consenso, il che può risultare sovente molto fastidioso per gli utenti; però, come ne conviene, affinché sia salvaguardata la privacy basta solo un pizzico di pazienza e la spendita di qualche secondo sufficiente a cliccare sulla voce "acconsento".

Inoltre affinché vi siano ulteriori garanzie il nuovo Regolamento ha sostituito gli obblighi più stringenti e vincolanti della precedente disciplina comunitaria, la Direttiva 95/46/CE, con il cosiddetto principio di *accountability*, ovvero il principio di responsabilizzazione. Ciò sta a significare che è il titolare del trattamento a doversi autonomamente adoperare per adottare tutte quelle misure e situazioni di matrice tecnico-organizzativa utili a dimostrare la conformità alle presenti norme regolamentarie[37]. Ancora meglio quando titolare e responsabile decidono spontaneamente di aderire a codici di condotta o meccanismi di autocertificazione, già discussi nel precedente capitolo.

Certo, non vi è un insieme di norme vincolanti in senso proprio, però allo stesso tempo il sistema sanzionatorio previsto dal Reg. 679/2016 si comporta come una sorta di incoraggiamento, per dirla con un eufemismo. Da una parte vi è la facoltà per gli Stati membri di ricorrere a sanzioni di tipo penale in base alla gravità della violazione, dall'altra l'ammontare delle sanzioni amministrative pecuniarie può raggiungere l'Everest dei 20 milioni di Euro annui oppure in alternativa il 4% del fatturato mondiale aziendale sempre annuo.

E proprio la possibilità di sanzionare una relativamente piccola percentuale del fatturato mondiale ci conduce a trattare un altro aspetto assai rilevante per la nuova disciplina europea: si ammette implicitamente l'eventualità di un trattamento di dati personali su scala non limitata magari alla mera nazione di stabilimento del titolare e/o del responsabile, bensì in modo ben più ampio geograficamente. Tale tipo di fattispecie implica il trasferimento dei dati verso paesi terzi extra-UE il che a sua volta risulta legittimo soltanto in presenza di determinate ipotesi.

---

[37] Cfr. Regolamento del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile. Art.24.

La Commissione europea deve innanzitutto valutare ed accertare se il paese terzo di destinazione garantisce un livello di protezione adeguato[38]; in base a quali parametri?

E' presto detto. Lo stato della legislazione è una variabile chiave: bisogna chiarire se sono previste dall'ordinamento "straniero" possibilità per gli interessati di eventuali ricorsi in sede amministrativa e giudiziaria in casi di violazione dei dati. Dopodiché deve essere effettivamente funzionante in loco una o più autorità di controllo garanti indipendenti e soprattutto competenti nel rispetto di possibili convenzioni o sistemi multilaterali internazionali in materia, evidentemente, di protezione di dati personali.

Può comunque configurarsi un caso di mancanza di decisione da parte della Commissione; in presenza di questa situazione il titolare o il responsabile potrà trasferire i dati verso un paese terzo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi[39].

Ma quindi quali sono queste fantomatiche garanzie adeguate che hanno la facoltà di esulare da specifiche autorizzazioni da parte delle autorità di controllo? Strumenti giuridicamente vincolanti e aventi efficacia esecutiva tra autorità pubbliche od organismi pubblici, norme vincolanti d'impresa[40], meccanismi di certificazione o adozione di codici di condotta e previsione di clausole di protezione dei dati approvate dalla Commissione. Infine al contrario costituiscono garanzie adeguate, ma bisognose di autorizzazione della autorità garante le clausole contrattuali tra titolare e/o responsabile mittenti con i loro "colleghi" destinatari e le disposizioni che vanno inserite in accordi amministrativi tra autorità pubbliche riguardo diritti effettivi ed azionabili per gli interessati.

Il DPO

Dulcis in fundo, novità di maggior rilievo per quanto riguarda l'ambito aziendale è sicuramente l'introduzione di una nuova figura professionale che va ad affiancarsi al titolare e al responsabile, ossia il responsabile della protezione dei dati, formalmente *data protection*

---

[38] In base al Regolamento il trasferimento di dati personali è ammesso se la Commissione europea ha deciso che il paese terzo o un territorio di esso garantiscono un livello adeguato di protezione.
Cfr. Regolamento del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile. Art.45.

[39] CICCIA MESSINA, A., e BERNARDI, N., 2016. *Privacy e Regolamento europeo.* Milano: Wolters Kluver Italia. Pag.64.

[40] Tali norme vincolanti d'impresa sono molto frequenti in casi di gruppi imprenditoriali che svolgono attività economiche comuni.

officer. Il DPO[41] dovrà essere presente in tutte le amministrazioni pubbliche ed enti pubblici, eccettuate le autorità giudiziarie, e anche presso tutte quelle aziende ed imprese che trattano dati su larga scala, che trattano dati sensibili e in quelle aziende per le quali è richiesto un sistematico e regolare monitoraggio degli interessati. E' ovvio che i soggetti non ricadenti in queste categorie legali possono comunque dotarsi autonomamente di un DPO, il che rivela uno spontaneo desiderio dell'impresa a conformarsi alla disciplina fornendo in questo modo maggiore trasparenza. Mentre, diverse società facenti parte di uno stesso gruppo, in prospettiva nazionale o transfrontaliera, potranno nominare un unico responsabile della protezione dei dati il quale deve essere facilmente raggiungibile da ciascuna società[42].

Il titolare del trattamento deve nominare come DPO un professionista che porti in serbo grande conoscenza della normativa e delle modalità di gestione dei dati personali, in modo del tutto indipendente e in assenza di qualunque tipo di conflitto di interesse. Su questo ultimo aspetto, però, è ravvisabile una piccola crepa: il data protection officer potrà assolvere i propri compiti da esterno alla azienda in base ad un contratto di servizi, quindi in totale assenza di conflitto di interessi, oppure potrà essere nominato tale essendo già un dipendente dell'impresa del titolare del trattamento. Questo ultimo caso può rappresentare un problema innanzitutto poiché in presenza di eventuali irregolarità il DPO è tenuto a "denunciare" la violazione, pena responsabilità dello stesso, ma così è come se si "autodenunciasse" dato che è dipendente della stessa azienda rea, dunque in conflitto di interessi. In secondo luogo potrebbero sorgere difficoltà relative alla disponibilità di risorse e di energie quando tale figura svolge già numerose attività o mansioni nel contesto della medesima azienda o di più aziende. Risulta, perciò, necessario trovare un equilibrio anche se non è per nulla semplice determinare a priori la quantità di risorse utili ad assolvere le funzioni previste dal ruolo di DPO.

---

[41] Sono gli Stati Uniti la culla di questa neonata figura in ambito europeo; nel 1999 la società californiana AllAdvantage istituì il "Privacy Offer" antesignano del DPO, ma sostanzialmente equivalente, ossia un avvocato specializzato in tutela della privacy.
MARINI, P., 2016. *Data Protection Officer: un super consulente in staff con la direzione aziendale.* Il Quotidiano Giuridico [on-line], 14 settembre.
Disponibile su: http://www.quotidianogiuridico.it/documents/2016/09/14/data-protection-officer-un-super-consulente-in-staff-con-la-direzione-aziendale [data di accesso: 13/06/2017].

[42] LESCE, D., e STUDIO LEGALE TRIFIRO'& PARTNERS, 2016. *Privacy: è iniziato il conto alla rovescia per le aziende.* Il Sole 24ore [on-line], 1 giugno.
Disponibile su: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-06-01/privacy-e-iniziato-conto-rovescia-le-aziende-110743.php [data di accesso: 14/04/2017].

E quali possono essere queste funzioni, questi compiti? Svolgere sicuramente attività di consulenza nei confronti di ogni soggetto all'interno dell'azienda circa gli obblighi derivanti dal Regolamento e quindi verificare la conformità ad esso, dopodiché fornire ove richiesto pareri riguardo la valutazione d'impatto sulla protezione dei dati e fungere da "punto di contatto" da una parte con gli interessati dall'altra con il Garante, nel caso italiano.

Teoricamente il DPO è funzione di *staff* con la direzione con compiti di supporto, consulenza, sorveglianza e interlocuzione con l'autorità di controllo, come già affermato; un professionista di alto livello che risponde solo al *top management.*

Un "organismo di vigilanza" in tema privacy. Sia chiaro però, questa figura è ad oggi ancora un'incognita per le aziende, è ancora del tutto teorica, ancora nell'Iperuranio, dato che attualmente i soggetti tenuti a munirsene sono sprovvisti.

Questo perché c'è molta confusione a livello normativo nazionale riguardo la concretezza del ruolo del DPO e la concretezza dei compiti da assegnarli, dal momento che l'autorità tenuta ad emanare le linee guida riguardo la disciplina della privacy, ovvero il Garante, ancora non si è espressa in modo chiaro ed univoco.

E', dunque, interessante osservare come evolverà la situazione una volta giunti sempre più in prossimità del termine di "recepimento" della disciplina regolamentaria fissato al maggio del 2018.

Curiosità, sicuramente, per l'aspetto più critico e delicato del tema, ossia la nomina del data protection officer: figura interna oppure esterna all'azienda, questo è il dilemma!

Conclusioni

Giunti alla foce della discussione, dunque, cosa ne rimane? Cosa resta di tutto l'insieme, di tutta la sfilza di provvedimenti, diritti, tutele, misure e contromisure? Leggendo le disposizioni del nuovo Regolamento il business man che opera nel contesto aziendale, il titolare di un qualsivoglia trattamento ed infine il soggetto interessato si sentono davvero al sicuro, protetti per quanto attiene alla sfera della privacy? In un' epoca in cui i dati personali e la privacy *tout court* hanno assunto un valore non soltanto intrinseco per gli interessati, bensì anche economico-aziendale preponderante, le norme del Regolamento sono probabilmente appena sufficienti a garantire la protezione dei dati personali. In un momento storico-sociale caratterizzato dal fatto che tali dati possono essere considerati il "petrolio" dell'oggi, il 679/16 di sicuro tende ad armonizzare la disciplina su tutto il suolo comunitario, ma contemporaneamente eccede nella semplificazione delle modalità di trattamento in modo da sgravare il carico di lavoro dalle piccole e medie imprese. Questo ultimo aspetto può ritenersi un piccolo campanello d'allarme: molti ambiti del Regolamento, alcuni di essi non toccati in questo elaborato per ragioni di semplicità, sono invero decisamente poco marcati ed ariosi. In questi si casi si rinvia all'interpretazione dei garanti nazionali sfumando in questo modo l'ideale di omogeneizzazione alla base del Regolamento stesso e portando quest'ultimo ad assumere quasi le sembianze di una vera e propria direttiva. Si prenda il caso di privacy by design e privacy by default: nella sostanza le imprese, le aziende cosa sono tenute a fare per essere conformi ai principi comunitari? Non è espressamente sancita nessuna regola pratica per così dire, nessun esempio concreto con cui le imprese possano confrontarsi e da cui possano prendere spunto, bensì si definisce soltanto il principio, l'idea del legislatore europeo. Si tratta di una fattispecie tipica della cosiddetta *soft law,* ossia un fenomeno di regolazione connotato dalla produzione di norme prive di efficacia vincolante diretta. Un limpido esempio è rappresentato anche dalle certificazioni, dai marchi di protezione dei dati o dai codici di deontologia: sono tutti meramente "incoraggiati" dal Regolamento, il che rivela una mancanza di obbligatorietà alla fonte.

In più il 679/16 sfiora appena aspetti quali il contesto lavoristico, come precedentemente accennato, e il diritto di espressione e di informazione, per i quali si rinvia al diritto proprio dei singoli Stati membri.

Sfortunatamente ad oggi tali questioni rimangono irrisolte e lo saranno fin quando il Garante italiano non stabilirà con precisione le modalità di attuazione dei neonati concetti europei da

calare nella realtà nazionale. Sino ad allora, come in un limbo, bisognerà rispettare le attuali norme, pur tenendo presente e cominciando ad apprendere ciò che avverrà nell'immediato futuro quando vi dovrà essere allineamento tra disciplina nazionale e comunitaria, avendo compreso come concretamente porsi nei confronti delle novità regolamentarie. Solo in quel momento si comprenderà se la nuova evoluzione dei presidi ai dati personali sarà davvero sufficiente a respingere le sfide ed i pericoli che giorno dopo giorno incrinano la sfera della privacy: se l'evoluzione dell'antidoto avrà tenuto il passo dell'evoluzione della malattia.

Totale parole: 13944.

Bibliografia

MONOGRAFIE:

ORWELL, G., 1949. *1984.* Milano: Mondadori.

WACKS, R., 2016. *Privacy Una sintetica introduzione.* 1^ed. Pescara: Monti & Ambrosini editori.

WESTIN, A. F., 1967. *Privacy and freedom.* New York: Atheneum. Pag.7.

CICCIA MESSINA, A., e BERNARDI, N., 2016. *Privacy e Regolamento europeo.* Milano: Wolters Kluwer Italia.

SITZIA, A., 2013. *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali.* Padova: Cedam.

BIAISOTTI, A., 2016. *Il nuovo regolamento europeo sulla protezione dei dati.* Roma: EPC editore.

PIZZETTI, F., 2016. *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo.* Torino: Giappichelli.

ARTICOLI WEB:

WARREN, S. L., e BRANDEIS, L. D., 1890. *The right to privacy.* Boston: Harvard Law Review.

Disponibile su: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [data di accesso:16/05/2017].

SCAFATI, G., e STUDIO LEGALE STELE' PERELLI, 2016. *La "privacy europea", il Regolamento UE 679/2016.* Il Sole 24ore [on-line], 16 maggio.

Disponibile su: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-05-16/la-privacy-europea-regolamento-ue-2016679-125453.php [data di accesso:14/04/2017].

LESCE, D., e STUDIO LEGALE TRIFIRO' & PARTNERS, 2016. *Privacy: è iniziato il conto alla rovescia per le aziende.* Il Sole 24ore [on-line], 1 giugno.

Disponibile su: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2016-06-01/privacy-e-iniziato-conto-rovescia-le-aziende-110743.php [data di accesso:14/04/2017].

SERRIELLO, A., 2016. *Quali dati personali sono considerati dati sensibili?* Unolegal Privacy Solutions [on-line], 7 settembre.

Disponibile su: http://www.unolegal.it/dati-personali-sono-dati-sensibili/
[data di accesso:30/05/17].

PANETTA, R., 2013. *Data breach: nuovo provvedimento del Garante Privacy sulle modalità di notifica.* Il Sole24ore [on-line], 10 maggio.

Disponibile su: http://www.diritto24.ilsole24ore.com/avvocatoAffari/mercatiImpresa/2013/05/data-breach-nuovo-provvedimento-del-garante-privacy-sulle-modalita-di-notifica.php [data di accesso: 30/05/17].

FONTI LEGISLATIVE:

Decreto Legislativo 30 giugno 2003, n° 196.

Regolamento del Parlamento europeo e del Consiglio n° 679/2016 del 27 aprile.

Legge 20 maggio 1970, n° 300 "Statuto dei lavoratori".

SLIDES:

GUERRA G., Avvocato. *Il nuovo Regolamento europeo sulla privacy: novità ed impatti per le attività di trattamento dei dati personali e gestione dei relativi adempimenti.*

BANCHE DATI ON-LINE:

LEGGI D'ITALIA [on-line]. Milano: Wolters Kluwer Italia.

Disponibile su: http://www.studiolegale.leggiditalia.it/#__name=main,__m=form

PUBBLICAZIONI GIURIDICHE:

MINAZZI, F., 2016. *Prima pronuncia del Garante contro Facebook.* Bruno e Ranieri Studio Legale Associato [on-line], 24 maggio. Disponibile su: http://www.studiolegalebrunoeranieri.it/facebook-e-privacy-prima-pronuncia-del-garante-privacy-contro-facebook/news/225/2016/5/26 [data di accesso: 13/06/2017].

FAMILIARI, S., 2017. *Un caso pratico di diritto all'oblio: la ricerca assistita di Google.* Il Quotidiano Giuridico [on-line], 6 marzo. Disponibile su: http://www.quotidianogiuridico.it/documents/2017/03/06/un-caso-pratico-del-diritto-all-oblio-la-ricerca-assistita-di-google

[data di accesso: 13/06/2017].

MARINI, P., 2016. *Oblio e portabilità dei dati: novità dal nuovo Regolamento Privacy europeo.* Il Quotidiano Giuridico [on-line], 26 luglio. Disponibile su: http://www.quotidianogiuridico.it/documents/2016/07/26/oblio-e-portabilita-dei-dati-novita-dal-nuovo-regolamento-privacy-europeo [data di accesso: 13/06/2017].

MARINI, P., 2017. *Regolamento europeo Privacy: i codici di condotta e le certificazioni.* Il Quotidiano Giuridico [on-line], 27 febbraio. Disponibile su: http://www.quotidianogiuridico.it/documents/2017/02/27/regolamento-europeo-privacy-i-codici-di-condotta-e-le-certificazioni [data di accesso: 13/06/2017].

MARINI, P., 2016. *Data Protection Officer: un super consulente in staff con la direzione aziendale.* Il Quotidiano Giuridico [on-line], 14 settembre. Disponibile su: http://www.quotidianogiuridico.it/documents/2016/09/14/data-protection-officer-un-super-consulente-in-staff-con-la-direzione-aziendale [data di accesso: 13/06/2017].