DATA PROTECTION LAW – RIVISTA GIURIDICA

Rivista online non soggetta ad obbligo di registrazione ai sensi dell'art. 3-bis del Decreto Legge 103/2012

Sito web: www.dataprotectionlaw.it

Contatti: info@dataprotectionlaw.it

"Data Protection Law" è una rivista elettronica di diritto Open access pubblicata dall'associazione Data Protection Law. La rivista pubblica con cadenza semestrale numeri costituiti da articoli scientifici inediti, saggi, traduzioni di estratti da opere scientifiche significative e di recente pubblicazione o articoli rilevanti per la comunità scientifica, recensioni di libri ed eventi culturali.
I numeri della rivista ospitano contributi scientifici prodotti e sottoposti su invito diretto della redazione.
Tutti i contributi sono sottoposti a doppia blind peer review.

Indice.

DATA PROTECTION IMPACT ASSESSMENT E SICUREZZA DEI DATI. NOVITÀ E CRITICITÀ ALLA LUCE DEL PRINCIPIO DI *ACCOUNTABILITY* NEL REGOLAMENTO UE PER LA PROTEZIONE DATI PERSONALI 679/2016.

Di Pamela La Farciola

SOMMARIO. 1. Valutazione d'impatto privacy e accountability. Riflessioni preliminari. – 2. Fonti della disciplina. – 3. Valutazione impatto privacy: quando effettuarla, quando è obbligatoria, relazioni con la verifica preliminare. – 4. Conclusioni.

The General Data Protection Regulation 679/2016 (GDPR) introduced the Data Protection Impact Assessment, one of the most important regulatory changes linked to accountability of data controller and data processor. This essay explores when a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of natural persons. In this case the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

1. Valutazione d'impatto privacy e *accountability*. Riflessioni preliminari

Dopo un lungo *iter* legislativo della durata di circa quattro anni, il 4 maggio 2016 è stato pubblicato sulla Gazzetta Ufficiale Europea il Regolamento UE n. 2016/679 sulla protezione dei dati personali[1], che in Italia sostituisce il precedente Codice della Privacy (D.lgs. n. 196/2003), a sua volta scaturito dalla c.d. "Direttiva madre" n. 95/46/CE.

[1] Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati).

Tale Regolamento si inserisce all'interno di quello che insieme alla Direttiva 2016/680[2] è stato definito il "Pacchetto europeo protezione dati".

Tra le novità più incisive introdotte dal *General Data protection regulation* (in seguito, GDPR), entrato in vigore il 25 maggio 2016 e divenuto pienamente applicabile dal 25 maggio 2018 in tutti gli Stati Membri dell'Unione europea, vi è la cosiddetta "valutazione di impatto privacy" (*Data Protection Impact Assessment*), che si inserisce nel più ampio contesto della responsabilizzazione (*accountability)* di titolari e responsabili nell'adozione di comportamenti cosiddetti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR[3].

Il principio di responsabilizzazione richiede al titolare del trattamento di porre in essere misure tecniche e organizzative adeguate per garantire, potendolo anche dimostrare, che il trattamento sia effettuato in modo conforme al GDPR[4].

Si tratta di un punto cruciale nel nuovo assetto previsto per la protezione dei dati in quanto è affidato ai titolari del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative vigenti, tenendo conto di alcuni criteri specifici indicati dal GDPR stesso.

Il primo fra tali criteri è sintetizzato nell'espressione inglese *Data protection by default and by design*, ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "*al fine di soddisfare i requisiti*" del GDPR e "*tutelare i diritti degli interessati*", considerando il contesto complessivo nel quale si inserisce il trattamento e i rischi per i diritti e le libertà degli interessati[5].

L'espressione *Privacy by design* indica proprio la necessità di contemplare la protezione dei dati fin dalla progettazione, ma anche obbligo di ridurre al minimo il trattamento dei dati personali mediante misure, sia tecniche che organizzative, quali ad esempio la pseudominizzazione dei dati personali. L'obiettivo da raggiungere è quello

---

2 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[3] artt. 23-25, in particolare, e l'intero Capo IV del GDPR 679/2016.

[4] E. ERRICHIELLO, *Il principio di responsabilizzazione e il suo antecedente nel Modello 231*, in *dataprotectionlaw.it*, 2018.

[5] Articolo 25, GDPR 679/2016 "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*".

di garantire che in fase di progettazione, sviluppo, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori interessati siano orientati a detto principio.

Privacy by default indica invece che la tutela della protezione del dato deve diventare l'impostazione predefinita, cosicché il titolare del trattamento dovrà adottare misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento in modo sostanzialmente predefinito. Gli obblighi valgono sia per la quantità dei dati personali raccolti, sia per il periodo di conservazione che per la portata del trattamento e l'accessibilità.

In sostanza, la tutela dei dati personali può avvenire solo attraverso una prefigurazione a monte delle azioni, iniziative, strumenti, procedure all'uopo necessarie, "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso"[6], richiedendo, un'analisi di tipo preventivo e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al criterio individuato dal GDPR rispetto alla gestione degli obblighi dei titolari, ossia il rischio che potrebbe essere generato dal medesimo trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati[7] e tali impatti dovranno essere

[6] *art. 25* del GDPR, cit.

[7] si vedano: Considerando n. 75 «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*»; Considerando n. 76 «*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*»; *Considerando n. 77: «Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può*

analizzati attraverso un apposito processo di valutazione[8], tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative, anche di sicurezza, che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto privacy, il titolare potrà decidere in autonomia se iniziare il trattamento ovvero, come alternativa, consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale.

Ma cos'è il rischio?

Le Linee-guida in materia di valutazione di impatto sulla protezione dei dati pubblicate dal Gruppo "Articolo 29"[9], fanno riferimento al rischio inteso come "*uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità*", e la gestione del rischio è ivi definibile "come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio".

Tra le molteplici definizioni a disposizione, si ritiene utile far riferimento anche all'art. 2, lettera s, D.Lgs. 81/2008[10]: "*rischio: probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione*".

In definitiva, il rischio è un concetto probabilistico, basato sull'ipotesi che accada un certo evento capace di causare un danno alle persone. La nozione di rischio implica però l'esistenza di una sorgente di pericolo e la possibilità che essa si trasformi in un danno.

Tale concezione di rischio, da sempre utilizzata nel linguaggio giuridico, trova origine nel diritto privato e prende le mosse da una attribuzione di valori che considera il rischio un evento futuro e incerto, certamente di tipo negativo, e che potrebbe generare un danno.

Partendo dal concetto di rischio e dalla logica costo-beneficio, si può ragionevolmente ipotizzare che anche nell'ambito della *data protection* potrebbe emergere una sorta di

---

inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio».

[8] si vedano artt. n. 35-36 GDPR.

[9] "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation*".

[10] Attuazione dell'articolo 1 della Legge 3 agosto 2007, n. 123 in materia di tutela della salute e della sicurezza nei luoghi di lavoro. (Gazzetta Ufficiale n. 101 del 30 aprile 2008 - Suppl. Ordinario n. 108).

nuovo modello, basato su una valutazione preventiva dei costi legati ad un sistema *compliance* con la disciplina sulla protezione dei dati personali e con conseguenti benefici in termini di guadagni e vantaggi.

Nella *data protection*, la logica costo-beneficio, può essere ricondotta alle teorie della c.d. monetizzazione dei diritti della personalità, di origine statunitense, secondo cui attribuendo ai dati personali un valore economico sia possibile effettuare una valutazione quantitativa del rischio e dell'eventuale danno.

1. Fonti della disciplina

La disciplina normativa sulla valutazione del rischio e di impatto privacy è prevista dall'articolo 35 del GDPR e dai Considerando 75,76,77,78.

Nella valutazione dei rischi si deve tenere conto delle eventualità di distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, e bisogna tenere conto degli eventuali pregiudizi che ne derivano: danni fisici, materiali e immateriali che posso coinvolgere i dati stessi.

Nel caso in cui i trattamenti presentino un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrà svolgere necessariamente una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. Qualora, però, tenuto conto delle tecnologie disponibili e/o dei costi di attuazione, non sia possibile l'adozione di misure di gestione del rischio elevato si dovrà consultare l'Autorità di controllo.

L'Autorità non assume il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive quali l'ammonimento del titolare o, più incisivamente, la limitazione o il divieto di procedere al trattamento.

Dunque, l'intervento delle Autorità di controllo è principalmente *ex post*, ossia successiva alle determinazioni assunte autonomamente dal titolare e ciò è in linea con la *ratio* supposta dal legislatore europeo volta all'eliminazione - con l'applicazione del Regolamento UE 679/2016 – di alcuni istituti previsti fin dalla direttiva del 1995 e dal Codice privacy italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare alla luce dell' art. 17 D.lgs.

30 giugno 2003, n. 196[11]), sostituiti nella nuova disciplina da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.

La tenuta del registro dei trattamenti risulta, pertanto, non soltanto un adempimento formale, bensì parte integrante di un sistema di corretta gestione dei dati personali.

Alle Autorità di controllo, e in particolare al Comitato europeo della protezione dei dati, spetta un ruolo finalizzato a garantire uniformità di approccio e a fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

È opportuno rilevare che "valutazione dei rischi" e "valutazione di impatto" sono istituti collegati ma differenti: la prima è sempre necessaria, come sempre è necessaria la sicurezza dei trattamenti; la "valutazione di impatto", viceversa, è attività riservata ai "rischi elevati" e presuppone il coinvolgimento, nelle ipotesi più delicate, dell'Autorità Garante. In ogni caso, è bene ricordare che la valutazione del rischio non costituisce una procedura completamente nuova, trattandosi di pratiche ben conosciute agli addetti ai lavori; pur tuttavia, con il GDPR si è avuta una formalizzazione normativa mediante un procedimento suggerito dal legislatore e non utilizzata solo per prassi.

A seguito dunque della previsione di un processo formalizzato di analisi del rischio, è necessario individuare *la ratio legis* alla base di tale previsione, che non è solo quella dell'*accountability* che vige nel GDPR, bensì anche quella della trasparenza.

Il binomio trasparenza-rischio risulta rinsaldato dal fatto che il principio della trasparenza, e per questa si intende anche la trasparenza e conoscibilità degli algoritmi alla base del procedimento, anticipa la valutazione del rischio. Ne consegue che una procedura pienamente trasparente porti ad una valutazione del rischio più efficace e maggiormente attendibile.

[11] Art. 17. Trattamento che presenta rischi specifici: 1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Il GDPR non prevede uno specifico elenco di misure di sicurezza, bensì riporta l'esemplificazione delle misure adeguate da adottare a seconda dell'analisi dei rischi/valutazione d'impatto.

I parametri a monte della individuazione delle misure sono le seguenti: lo stato dell'arte, i costi di attuazione, la natura, l'oggetto, il contesto e le finalità del trattamento, il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure possono essere tecniche e organizzative e tra queste: la pseudonimizzazione e cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il livello di sicurezza può considerarsi adeguato quando è in grado di contrastare i rischi contemplati nel Considerando n. 75, come la distruzione; perdita; modifica; divulgazione non autorizzata; accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati; discriminazione, furto o usurpazione d'identità; perdite finanziarie, pregiudizio alla reputazione, decifratura non autorizzata.

3. Valutazione impatto privacy: quando effettuarla, quando è obbligatoria, relazioni con la verifica preliminare

La valutazione di impatto privacy, unitamente agli altri adempimenti formali previsti (es. tenuta dei registri del trattamento), si può intendere come sostituzione dell'obbligo generale di notificare alle Autorità di controllo il trattamento dei dati personali che, come detto, si inserisce nel principio della responsabilizzazione del trattamento che impernia l'intero Regolamento UE: il GDPR sceglie delle strategie di tutela di natura sostanziale, incentrate sulla valutazione d'impatto, soprattutto con riferimento a trattamenti che comportano l'utilizzo di nuove tecnologie.

La valutazione di impatto privacy, come già accennato, deve essere effettuata precedentemente al trattamento, per poter soppesare la particolare probabilità e gravità del

rischio, tenendo conto che proprio mediante tale valutazione si acquisiscono le necessarie conoscenze sulle misure, sulle garanzie e sui meccanismi previsti per attenuare il rischio e assicurare la conformità del trattamento agli standard normativi.

La valutazione d'impatto è richiesta in particolare ai trattamenti su larga scala, che implicano una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale, il cui trattamento presenta un rischio potenzialmente elevato per l'incidenza ricadente su un rilevante numero di soggetti interessati.

Sulla questione della c.d. "larga scala", non è chiaro cosa si intenda effettivamente con questa espressione, nonostante le indicazioni fornite dalle linee-guida Gruppo articolo 29 che raccomanda di tenere in considerazione determinati parametri quali "1. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; c. durata, o persistenza, dell'attività di trattamento; d. ambito geografico dell'attività di trattamento".

Perplessità sorgono in relazione al fatto che i trattamenti su "larga scala" potrebbero riguardare, per esempio, i dati trattati in una struttura ospedaliera ma non quelli trattati dal singolo medico di famiglia. E allora ci si potrebbe chiedere: siamo certi che i dati trattati da un medico di base che ha 500 pazienti non siano da ritenersi su larga scala?

La valutazione d'impatto viene richiesta anche nei casi in cui i dati personali vengono trattati in funzione dell'adozione di decisioni riguardanti determinate persone fisiche in seguito ad una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e a reati o connessi a misure di sicurezza.

Alla luce di quanto sopra delineato, risulta evidente la ragione per cui il GDPR assegna all'Autorità garante il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati e anche un elenco delle tipologie di trattamenti per le quali la stessa non è richiesta.

Per quanto riguarda il procedimento da adottare, bisogna considerare che il titolare del trattamento, qualora svolga una valutazione di impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, eventualmente designato. La valu-

tazione deve contenere alcuni elementi, quali la descrizione chiara, esaustiva e sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, l'interesse legittimo perseguito dal titolare del trattamento; l'analisi della necessità e proporzionalità dei trattamenti in relazione alla finalità; la stima dei rischi per i diritti e le libertà degli interessati; le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone eventualmente implicate.

È utile ancora rilevare come il GDPR preveda che il titolare effettui il costante monitoraggio dei trattamenti in relazione ad eventuali variabili intervenienti che possono modificare l'incidenza e la stima del rischio per la protezione dei dati.

Si possono talvolta verificare dei casi in cui il rischio per la protezione dei dati non possa essere ragionevolmente attenuato mediante l'uso delle tecnologie disponibili o anche per gli elevati costi di attuazione, così da rendere necessaria la consultazione dell'Autorità di controllo prima dell'inizio delle attività di trattamento.

L'impostazione del GDPR si fonda infatti sul principio che "*si è conformi se si è sicuri*" e alla base di ciò vi è il compito del titolare del trattamento di dimostrare di esserlo.

È tuttavia da rilevare che tale principio non risulta una novità assoluta, dato che il D.lgs. n. 196/2003, all'art 15 "*Danni cagionati per effetto del trattamento*"[12], equiparando il trattamento dei dati personali allo svolgimento di un'attività pericolosa, prescrive proprio al titolare dei dati l'onere di dimostrare il proprio livello di sicurezza. Il Codice civile, all'articolo 2050, afferma che "chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".

La capacità di effettuare una adeguata analisi preliminare o di dimostrare a posteriori il proprio livello di sicurezza, e dunque anche di conformità, risulta essere una necessità ineludibile, che richiede l'uso di adeguati modelli di analisi e di gestione. L'obiet-

[12] Art. 15 Danni cagionati per effetto del trattamento: "*1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11*".

tivo sarebbe quello di abbandonare il tradizionale modello passivo, basato sulla concezione di "*regole da rispettare*", per giungere ad un modello attivo, basato su una gestione proattiva del rischio, che si ponga la questione di "*quali obiettivi raggiungere*", andando a definire in modo chiaro la direzione che si vuole prendere, e cioè il risultato che si vuole ottenere unitamente al rischio che ragionevolmente può considerarsi accettabile. Da qui, la pianificazione di azioni che potrebbero incrementare la responsabilità (*accountability*) ed arrivare a un contenimento dei costi e a possibili vantaggi competitivi, oltre che ad una maggiore tempestività nell'individuazione e nella gestione delle nuove emergenti minacce.

Le linee Guida in materia si basano sulla procedura di valutazione del rischio, mediante la quale si dovrebbe realizzare il tentativo di andare al di là della dimensione individuale della protezione dei dati, proiettandosi sulla dimensione collettiva dell'utilizzo degli stessi, come sostiene fermamente il Professore Alessandro Mantelero del Politecnico di Torino[13]. In questa prospettiva, i potenziali pregiudizi presi in esame in termini di tutela non sono circoscritti ai tipici rischi, ma guardano anche a pregiudizi di differente natura, in specie al potenziale conflitto fra impiego dei dati e valori etici e sociali, considerando per esempio i rischi di discriminazione sociale, in linea con il modello PESIA (*Privacy, Ethical and Social Impact Assessment*).

In tale ottica, il diritto del singolo ad avere il controllo sui propri dati personali e sul relativo trattamento, riconosciuto dalla Convenzione 108, evolve in una più ampia nozione di controllo, ove il controllo individuale trova completamento in un processo più complesso di valutazione del rischio concernente i molteplici impatti negativi che possono comportare l'impiego dei dati e la rappresentazione della nostra società attraverso gli algoritmi[14].

Punto cruciale e critico nel condurre una valutazione dell'impatto dell'uso dei dati in termini etici e sociali è costituito dall'individuazione dei valori che dovrebbero ispirare l'utilizzo dei dati; tali valori necessitano però di una contestualizzazione e sono difficili da individuare in modo assoluto o oggettivo, poiché rispecchiano le differenti tradizioni culturali esistenti.

[13] A. MANTELERO, *Il Consiglio d'Europa adotta le prime linee guide internazionali su Big Data e tutela dei dati personali*, in *Diritto Mercato Tecnologia*, Ministero dei Beni e delle Attività Culturali e del Turismo, 21 febbraio 2017.
[14] Ibidem

A tal fine, le Linee guida citate in precedenza delineano un tipo di architettura a tre livelli. Il primo, più generale ed elevato, mira ad individuare i "valori etici guida comuni" che dovranno costituire la base della valutazione d'impatto. Questi valori sono rinvenibili nelle carte internazionali dei diritti umani e delle libertà fondamentali, quali la Convenzione europea per la salvaguardia dei diritti dell'uomo. In tali carte si trova, infatti, il minimo comune denominatore degli approcci seguiti nei diversi Paesi[15]. Un secondo livello, laddove trovano maggiore specificazione i parametri valutativi di riferimento ora menzionati, tiene invece conto della natura dipendente dal contesto dell'impatto sociale ed etico dell'uso dei dati. In questa prospettiva, nelle linee guida si afferma che l'impiego dei dati personali non deve essere in conflitto con i valori etici comunemente riconosciuti e che il trattamento dati non deve pregiudicare "interessi sociali, valori e norme"[16]. Infine, le linee guida combinano questi suggerimenti di carattere generale con un'opzione maggiormente incentrata sulle specificità del singolo impiego dei dati e, a tal livello di dettaglio, ravvisano in comitati etici costituiti *ad hoc* lo strumento utile per identificare i valori specifici da salvaguardare nel caso concreto, fornendo una guida più dettagliata per la valutazione del rischio[17].

Le linee guida indicano che la valutazione dei rischi "dovrebbe essere effettuata da persone con adeguata qualificazione professionale e con le conoscenze per valutare i diversi impatti, tra cui le dimensioni legali, sociali, etiche e tecnologiche".

La dimensione collettiva del potenziale impatto dell'uso dei dati dovrebbe indurre a un approccio capace di coinvolgere i vari *stakeholders*, così da riuscire a dare voce ai diversi gruppi di persone che possono essere colpite da un determinato utilizzo dei dati e quindi da ritenersi portatrici di interesse.

Da uno sguardo attento emerge chiaro l'immediato affiancamento della DPIA all'attuale verifica preliminare prevista dal Codice della Privacy, all'art. 17. In un'ottica di responsabilizzazione dei titolari del trattamento, la DPIA potrebbe essere vista come una sorta di auto-verifica preliminare che ciascun titolare debba svolgere autonomamente per avere contezza di quali siano i rischi che il trattamento dei dati comporta[18]. Solo quando, effettuata la valutazione di impatto privacy, sia presente un alto rischio

[15] Ibidem
[16] Ibidem
[17] Ibidem
[18] Osservatorio Privacy, DPIA e verifica preliminare, *Riflessioni in seguito alla pubblicazione delle prime linee guida sulla valutazione d'impatto privacy*, in Il Sole 24 Ore del 26 aprile 2017.

residuo per le attività di trattamento dati, il titolare può chiedere all'autorità Garante di pronunciarsi in merito al trattamento in questione, richiedendo una consultazione preventiva. La DPIA, per come è concepita e descritta nelle linee guida, si discosta molto da quella che è l'attuale disciplina della verifica preliminare ex art. 17 d.lgs. 196/2003. La valutazione d'impatto, infatti, sembra essere focalizzata prevalentemente su un'analisi dello strumento tecnologico in uso, piuttosto che sulle criticità del trattamento in generale. Viceversa, l'attuale verifica preliminare ricomprende non solo un'attenta analisi tecnica, ma anche una precisa e puntuale contestualizzazione degli strumenti tecnologici utilizzati, correlati di volta in volta al caso specifico.

Ci si domanda allora se dal 25 maggio 2018 la verifica preliminare sia stata davvero sostituita dalla DPIA.

La possibilità di generalizzare e ampliare la portata della DPIA mal si concilia con la necessità, a DPIA conclusa, di eseguire l'analisi, questa volta puntuale, del rischio specifico residuo, necessario al fine di chiedere la consultazione preventiva ex art. 36 GDPR all'autorità Garante. Cioè, a fronte di un medesimo strumento tecnologico e di un'unica DPIA, la diversificazione dei casi concreti dei trattamenti si riflette inevitabilmente sulla valutazione preventiva del rischio, non potendosi trascurare quelle particolarità e specialità di ogni singolo trattamento, che spesso costituiscono i fattori di maggiore rischio.

Si può riprendere l'esempio fatto nelle linee guida a dimostrazione del fatto che per quanto identico possa essere lo strumento tecnologico installato (ed oggetto di DPIA), potrebbe essere diverso il rischio derivante dal suo utilizzo: l'installazione di telecamere presso una stazione vicina ad una scuola o a un ospedale comporta necessariamente rischi diversi e maggiori, che devono essere considerati singolarmente e in modo circostanziato[19].

Il Garante italiano, al fine di agevolare il titolare nell'ambito dell'identificazione dei casi in cui è opportuno procedere con una DPIA, ha fornito un ulteriore supporto operativo, pubblicando il 15 novembre 2018 un provvedimento avente carattere generale

[19] Cfr. Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "*possa presentare un rischio elevato*" ai sensi del regolamento 2016/679 (17/EN WP 248).

e riguardante l'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Il base a tale provvedimento, emanato ai sensi dell'art. 35, comma 4, del GDPR, ogni autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica, in seguito, tali elenchi al comitato di cui all'articolo 68 del citato Regolamento.

Attraverso questa facoltà concessa dal GDPR, le *Supervisory Authority* degli Stati membri possono creare propri elenchi.

Il Garante italiano ha provveduto a stilare il proprio elenco e a comunicarlo all'EDPB (*European Data Protection Board*) che, a sua volta, nella *Opinion 12/2018*, ha specificato il *framework* di tale intervento.

Sulla base delle indicazioni ricevuta dal *Board* europeo, il Garante italiano ha provveduto, quindi, ad individuare dodici casistiche in presenza delle quali la DPIA deve essere considerata obbligatoria: 1. Trattamenti valutativi o di *scoring* su larga scala, trattamenti che comportano la profilazione degli interessati, nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato; 2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono effetti giuridici oppure che incidono in modo analogo significativamente sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi); 3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione (inclusi servizi web, tv interattiva, etc.) rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati (ad es. in ambito telecomunicazioni, banche, etc.) effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget,

di upgrade tecnologico, miglioramento reti, offerta di servizi anti-frode, anti-spam, sicurezza etc.; 4. Trattamenti su larga scala di dati aventi carattere estremamente personale (WP 248, rev. 01). Tale categoria fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione), oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti); 5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (compresi i sistemi di video-sorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (v. WP 248, rev. 01, sui criteri nn. 3, 7 e 8); 6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo); 7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01; 8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche; 9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment); 10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse; 11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento; 12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

4. Conclusioni

In base al GDPR, l'inosservanza degli obblighi concernenti la DPIA può comportare l'imposizione di sanzioni pecuniarie da parte della competente autorità di controllo.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3 - 4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi

2 e 7-9) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (art. 36, paragrafo 3, lettera e) possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero, se si tratta di un'impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

In ogni caso, come suggerito dalle linee guida, il messaggio ultimo di tale disciplina è rappresentato dal fatto che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. Partendo da tale presupposto, la valutazione di impatto permette di realizzare concretamente anche l'altro fondamentale principio fissato nel regolamento europeo 679/2016, ossia la protezione dei dati fin dalla fase di progettazione di qualsiasi trattamento e la responsabilizzazione dello stesso titolare.

Molte questioni rimangono tuttavia ancora aperte ed esse richiederanno una sufficiente sperimentazione pratica che, ancora al momento, non risulta sufficiente per compiere una realistica analisi di bilancio su quanto finora sperimentato.

Al di là delle soluzioni concrete e dei tecnicismi che gradualmente si svilupperanno, dal quadro complessivamente delineato, emerge una importante evoluzione giuridica e culturale in atto, che parte dalla consapevolezza della centralità del tema della responsabilizzazione nel suo complesso e che vede consolidarsi il diritto fondamentale alla protezione dei dati personali attraverso una sua progressiva e crescente affermazione sul piano giuridico formale e sostanziale.

LA PROTEZIONE DEI DATI PERSONALI NEL CONDOMINIO.

di Giovanna Laurino

SOMMARIO. 1. Premessa. 2. Il rapporto tra Regolamento Europeo e la normativa condominiale. 3. Il trattamento dei dati tra minimizzazione e consenso. 4. Il Registro di anagrafe condominiale tra diritto di accesso e riservatezza. 5. La videosorveglianza condominiale. 6. Conclusioni.

Once the European Regulation 678/16 came into effect, it has been a significant impact on the companies'life, public institutions, and more generally on all those subjects that deal with personal data and needed to review their internal personal data protection policies to adapt them to the guarantees prescribed by the European legislator. Concerning the co-owners the need for managing the common good in transparency and efficiency it must be combined with the protection of the involved individuals' rights. Therefore, the duties to be carried out by the co-owners, are enhanced with respect to those already established by the sector legislation, so it will be necessary to prepare an appropriate disclosure statemen in accordance with GDPR, to draw up a register of the treatments and to respect the rights of the interested parties. Finally the Condominium manager must proceed, for each personal data processing, according to full transparency and data privacy protection.

1. Premessa.

Il Regolamento Generale n. 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali incrocia la propria esistenza con una pluralità di ambiti, compreso quello condominiale, prescrivendo per i soggetti che in tali contesti operano di impostare e/o adeguare la propria gestione della privacy nella direzione di un approccio al rischio fondato essenzialmente sul principio dell'*accountability*.

Tutto ciò comporta che il Titolare del trattamento, nell'ambito della propria autonomia, ha l'obbligo di dimostrare di aver adottato un processo complessivo di misure

giuridiche, organizzative e tecniche per la protezione dei dati e che i trattamenti effettuati siano adeguati e conformi alla normativa europea.

Inoltre, la corretta attuazione della disciplina necessita di una definizione puntale dei ruoli privacy, oltre che di una approfondita conoscenza del contesto informatico e giuridico, che ben potrebbe richiedere, ove non obbligatoriamente previsto, il supporto di una nuova figura professionale denominata *Data Protection Officer*.

In questa ottica, quindi, dovranno essere interpretati ed applicati gli istituti di nuova previsione, quali il Registro del trattamento e la valutazione preventiva di impatto.

In buona sostanza, nella prospettiva della cd. *data protection privacy by design* e *by default*, secondo le quali la protezione dei dati deve essere prevista in fase di progettazione e di studio di nuove attività di trattamento, oltre che realizzata quale impostazione predefinita, anche il Condominio è chiamato ad applicare, per ciascun trattamento messo in atto, la disciplina europea e a ricercare un costante equilibrio tra trasparenza dell'attività di gestione delle parti comuni e riservatezza delle informazioni personali, impattando inevitabilmente nel diritto di accesso dei condomini-interessati.

2. Il Rapporto tra Regolamento europeo e la normativa condominiale

All'indomani dell'entrata in vigore del Regolamento europeo n.679/2016, tutti i soggetti che si occupano, seppure indirettamente, di dati personali, quali società, Enti pubblici e associazioni private, sono stati chiamati a rivedere le politiche interne di gestione della privacy delle proprie realtà organizzative per adeguarle alle garanzie richieste dal legislatore.

I dati personali, definiti alla stregua dell'art. 4 del Regolamento come *"...qualsiasi informazione riguardante una persona fisica identificata o identificabile*…", sono la risorsa più preziosa delle economie contemporanee e, pertanto, la consapevolezza delle modalità di impiego delle informazioni, unitamente all'affermazione dei diritti azionabili dai soggetti interessati, dovrebbe rappresentare un primo freno alla realizzazione del controllo e della profilazione di massa, oltre che impedire un uso distorto dei dati personali.

Allo stesso tempo, una gestione attenta di tali dati avrebbe quale risvolto immediato la conoscenza più accurata delle problematiche e dei rischi connessi al trattamento illegittimo e alla diffusione non autorizzata delle informazioni personali.

La normativa si rivolge proprio a quei soggetti che effettuano un trattamento dei dati personali, inteso, ai sensi dell'art. 4 del GDPR, come *"…qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto, la limitazione, la cancellazione o la distruzione…",* i quali dovranno proteggere le informazioni personali a prescindere dalla tecnologia o dalle tecniche impiegate per il trattamento.

Infatti, la relativa disciplina troverà applicazione nei casi di trattamento automatizzato e manuale, purché i dati personali siano contenuti o destinati ad essere contenuti in un archivio (considerando 15), ossia, ai sensi dell'art. 4 n. 6 del GDPR, in un *"…qualsiasi insieme strutturato di dati personali accessibili secondo dei criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico."*.

In tale prospettiva, può dirsi che anche il Condominio, sia sotto il profilo soggettivo che oggettivo, rientra perfettamente nel novero dei soggetti tipizzati dal legislatore europeo, in quanto, seppure per altre ragioni e differenti finalità, si trova a dover maneggiare un gran quantitativo di dati personali e a porre in essere quelle attività definite trattamento alla stregua del Regolamento europeo

Invero, se in epoca romana, l'insulae si componeva di tre o quattro piani in cui risiedevano poche famiglie, successivamente, la seconda rivoluzione industriale ha visto la diffusione di condominii che, nelle periferie delle città hanno occupato, prima ampi spazi orizzontali, per poi divenire moderne torri di Babele, fino ad assistere, ai giorni nostri, alla nascita del cd. supercondominio, una "federazione" di più condominii, vera e propria città all'interno delle città.

L'ampliarsi degli edifici, dunque, ha determinato un aumento di informazioni personali, anche di natura particolare, che transitano all'interno del condominio.

Sotto un profilo propriamente tecnico-giuridico, il cd. Condominio degli edifici si delinea quale particolare forma di comunione, in cui proprietà esclusive coesistono con proprietà comuni. Tale istituto si configura allorquando sussistono più unità immobiliari in cui convive una proprietà individuale relativa ai piani o porzioni di piano

di cui sono titolari in modo esclusivo i singoli condomini, e una comproprietà degli stessi sui beni comuni, tra loro strutturalmente e funzionalmente collegate. Il rapporto che intercorre tra questi due diversi insiemi di beni è, anche secondo una giurisprudenza consolidata, quello di strumentalità o vincolo di accessorietà, per cui "*…il condominio si basa sulla relazione di accessorietà tra i beni comuni e le proprietà individuali".*[20]

In presenza di tale situazione strutturale, oltre che giuridica, troverà applicazione, per quanto non espressamente previsto dalla disciplina speciale, dagli artt.1117-1339 c.c., la normativa in materia di comunione.

Il condominio viene considerato, anche a seguito dell'entrata in vigore della Legge 220/2012, non come un soggetto giuridico dotato di una propria personalità distinta da quella di coloro che ne fanno parte, bensì quale ente di gestione caratterizzato da una forte soggettività, che opera in rappresentanza e nell'interesse comune dei partecipanti, limitatamente all'amministrazione e al buon uso della cosa comune senza interferire nei rapporti autonomi di ciascun condomino.

Ne deriva che l'amministratore, per effetto della nomina ex art. 1129 c.c., si configura come un soggetto distinto dalla compagine condominiale, il quale ha soltanto una rappresentanza *ex mandato* dei vari condomini, la cui presenza non priva questi ultimi del potere di agire personalmente a difesa dei propri diritti esclusivi e comuni.

In tal senso, può dirsi che la fonte dei poteri è da rinvenirsi nel contratto di mandato, in virtù del quale, una volta conferito l'incarico, si determina in capo all'amministratore la nascita degli obblighi tipizzati, derivanti direttamente dall'art. 1129 c.c. e dalla leggi speciali, oltre a quelli direttamente desumibili dalla posizione di mandatario e collegati alla corretta gestione della vita condominiale e dei beni comuni.

Pertanto, agli obblighi nascenti dall'art. 1130 c.c., si accompagna il generale dovere di diligenza ex art. 1710 che si estende a tutti gli atti compiuti nell'esecuzione dell'incarico, ivi compresi gli atti preparatori e strumentali.

Rientrano tra i compiti dell'amministratore:

1) eseguire le deliberazioni dell'assemblea condominiale e far rispettare le norme del regolamento;

[20] Cassazione civile 21 settembre 2012, n. 16128.

2) vigilare sull'uso delle cose comuni e la prestazione dei servizi comuni;

3) provvedere alla riscossione dei contributi e al pagamento delle spese occorrenti per la manutenzione ordinaria delle parti comuni e dell'edificio e per i servizi comunali;

4) provvedere agli atti conservativi dei diritti sulle parti comuni dell'edificio;

5) rendere conto della gestione ogni anno.

Oltre a tali attribuzioni, tradizionalmente riconducibili all'attività dell'amministratore, la novella del 2012 ha introdotto ulteriori adempimenti prevedendo: l'obbligo espresso di convocazione annuale dell'assemblea per la presentazione del rendiconto con indicazione di un termine di giorni 180 per la presentazione; il dovere di eseguire adempimenti fiscali, l'obbligo di curare la tenuta del registro dell'Anagrafe Condominiale, con specificazione del relativo contenuto e la previsione di obblighi a carico dei condomini finalizzati ad un continuo aggiornamento dei dati trattati; l'obbligo di curare la tenuta del Registro dei Verbali che comprende anche la redazione del cd. verbale di diserzione, e la registrazione delle dichiarazioni dei singoli condomini; obbligo di tenuta del Registro di Contabilità.

A ciò deve aggiungersi l'obbligo di conservazione di tutta la documentazione inerente alla gestione del condominio, comprensiva di quella concernente le condizioni tecnico/amministrative dell'edificio, oltre al dovere di fornire al singolo condomino che ne faccia richiesta le opportune attestazioni in ordine allo stato dei pagamenti e delle pendenze giudiziali.[21]

A ben guardare, il Regolamento generale sulla protezione dei dati, entrato effettivamente in vigore nel 2018, dopo un periodo di transizione, interviene non nel senso di modificare la normativa nazionale, ivi compresa quella condominiale, che rimane la stessa, ma al solo fine di fissare regole più stringenti sia per quanto riguarda il trattamento dei dati personali e sia per quanto concerne la realizzazione della trasparenza nella gestione condominiale, che coinvolge le fasi di diffusione e/o comunicazione a terzi delle informazioni personali.

Al contempo la normativa europea impone chiarezza di ruoli e di organizzazione e quindi, per poter funzionare correttamente necessita di un organigramma ben definito

[21] CARINGELLA-BUFFONI, *Manuale di diritto Civile,* Roma, 2015, p.464

e di relative nomine ed incarichi, che possono essere gestiti in parallelo a funzionigramma già in atto.

Pertanto, il processo di adeguamento anche in ambito condominiale, deve tener conto delle significative innovazioni con cui il legislatore europeo, indicando le condizioni regolative essenziali della legittimità del trattamento tanto nell'*an,* (presupposti di legittimità, basi giuridiche), quanto nel *quomodo,* (condizioni di ammissibilità e modalità di realizzazione del trattamento), ha inteso uniformare la disciplina della protezione dei dati negli ordinamenti dei singoli Stati membri.

Di qui l'operare di una serie di principi volti a rendere uniforme ed effettiva la protezione dei dati personali fra cui l'*accountability*, che informa l'intero nuovo quadro giuridico europeo, e l'espressa introduzione del principio di trasparenza, per effetto della quale, ai sensi dell'art. 5 lett. a) del GDPR *"i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*".

Essi descrivono la cornice essenziale al cui interno la normativa di protezione dei dati si sviluppa, ed in tal modo, mentre la liceità assolve la funzione di selezionare i presupposti legittimanti il trattamento, in base al bilanciamento realizzato tra il diritto alla protezione dei dati personali e gli interessi potenzialmente confliggenti, la correttezza attiene al rapporto tra il titolare e l'interessato, con risvolti evidenti per l'intera collettività e, unitamente alla trasparenza, rappresenta un presupposto indispensabile per la realizzazione della cd. autodeterminazione informativa. La correttezza, quindi, deve ispirare, nei canoni della lealtà e della buona fede e del limite dell'abuso del diritto, la condotta del titolare, mentre la trasparenza, alla stessa complementare, è diretta essenzialmente a rendere l'interessato consapevole delle caratteristiche del trattamento.

La ricaduta pratica dell'applicazione del principio di responsabilizzazione appare in tutta evidenza nella previsione che riguarda il titolare del trattamento (*data controller*), ossia ex art. 4 del GDPR *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali",* il quale, ai sensi dell'art. 24 gdpr, viene chiamato a mettere *"... in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento".*

Tali misure, così come specificato nel considerando 74, devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone interessate[22].

In buona sostanza, nella nuova prospettiva della cd. privacy *by design e by default*, la protezione dei dati personali non potrà essere trascurata o sottovalutata né in fase di progettazione iniziale di sistemi di trattamento e né nei successivi funzionamenti e sviluppi, e dovrà diventare impostazione predefinita. Pertanto, il titolare provvede non solo ad incorporare la tutela della privacy in tutto il ciclo di attività del trattamento dei dati, sin dalla fase iniziale di progettazione, minimizzando la raccolta dei dati e i relativi trattamenti, ma prevede, altresì, un utilizzo dei dati che sia limitato ai soli casi necessari per ogni specifica finalità di trattamento.

Il titolare del trattamento e, per esso in ambito condominiale l'Amministratore, deve essere in grado di dimostrare la predisposizione e l'aggiornamento di misure adeguate alla tutela dei dati. In particolare, egli deve essere in grado di provare di aver adottato un processo complessivo di misure giuridiche, organizzative, tecniche, anche attraverso l'elaborazione di specifici modelli organizzativi, e deve poter dimostrare in modo positivo e proattivo che i trattamenti di dati effettuati siano adeguati e conformi al regolamento europeo.

Così, volendo dare un concreto riscontro applicativo della normativa, essa non pare più consentire, ad esempio, che le comunicazioni da parte dell'Amministratore ai condòmini, contenenti indicazioni di dati personali degli stessi, compresi i verbali di assemblea, possano essere trasmessi mediante semplice e-mail, tantomeno se indicante, nella relativa intestazione, l'indirizzo e-mail del complesso dei destinatari.

Di contro, le esigenze di sicurezza potranno essere soddisfatte attraverso il loro caricamento su un sistema informatico che garantisca, attraverso l'utilizzo di *username* e una *password*, l'identità dei soggetti che entrano in possesso di tali dati. L'invio di email o di eventuali raccomandate potrà informare i condòmini destinatari dell'avvenuto caricamento a sistema dei dati e l'invito ad accedervi utilizzando username e password precedentemente comunicati.

[22] GDPR E NORMATIVA PRIVACY COMMENTARIO, a cura di RICCIO, SCORZA, BELISARIO, Milano, 2018, p.1-100.

In caso di tenuta di dati in formato elettronico si dovrà prevedere l'utilizzo di idonei sistemi antivirus che prevengano *data breach*, come pure, in caso di tenuta dei dati in formato cartaceo, l'utilizzo di luoghi idonei e protetti dal pubblico.

Nell'ottica del GDPR, diversamente da quanto previsto nella previgente normativa, si pone l'accento innanzitutto sulla tempistica dell'attenzione alla protezione dei dati, passando da una regolamentazione volta a determinare i rimedi alle possibili violazioni e ai danni conseguenti, con forte connotazione reattiva, ad una legislazione rivolta verso una protezione preventiva ed effettiva. Invero, piuttosto che sulla ricerca *ex post* del rimedio, il legislatore europeo ha inteso costituire un sistema di protezione basato sulla valutazione preventiva, sull'esame prudenziale di tutte le attività di trattamento.

Pertanto, in tale interpretazione oggetto della prova non è essere soltanto l'*an* dell'adozione delle misure richieste, che non sono più indicate nel minimo dal legislatore, ma il *quomodo* e il *quantum,* oltre al fatto che i riscontri dovranno riguardare l'adeguatezza delle misure effettivamente adottate rispetto ai rischi connessi ai trattamenti[23].

Analoga impostazione può dirsi sussistente anche per il Responsabile del trattamento, *o data processor*, il quale indicato al par. 1 n. 8 dell'art. 4 GDPR, come *" la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento"*, ove previsto, viene ad essere gravato, in solido con il titolare, di una serie di obblighi e chiamato a rispondere dei danni causati laddove non abbia adempiuto ai dettami nascenti dal Regolamento ovvero abbia agito in modo contrario e difforme rispetto alle istruzioni ricevute dal titolare del trattamento.

La declinazione in ambito condominale dei suddetti principi, oltre a comportare la ricerca di un costante bilanciamento tra gli obblighi di trasparenza ai fini della corretta gestione condominiale e il rispetto della riservatezza dei singoli condomini, onera l'amministratore, che nell'esercizio delle sue funzioni viene in possesso di dati personali, ad un utilizzo per finalità determinate, esplicite e legittime e successivamente per i soli scopi compatibili con tali finalità.

Inoltre, è previsto che i dati personali trattati devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità per cui sono stati acquisiti; gli stessi devono

[23] *Op. cit*, a cura di RICCIO, SCORZA, BELISARIO, Milano, 2018, p.62.

essere esatti e, se necessario, aggiornati; conservati in modo che sia consentita l'identificazione degli interessati per un tempo limitato al conseguimento degli obiettivi per cui sono raccolti; trattati con modalità idonee a garantirne la integrità e la sicurezza, attraverso l'utilizzo di misure tecniche e organizzative adeguate, che ne proteggano il contenuto da trattamenti non autorizzati o illeciti.

Pertanto, accanto al compimento degli adempimenti già previsti dal codice civile, la normativa europea prescrive per il titolare del trattamento ulteriori e specifiche attività che si sostanziano nella predisposizione dell'informativa, ex art. 13-14 Gdpr, con cui l'interessato dovrà essere edotto delle caratteristiche essenziali del trattamento; nell'obbligo di tenuta del registro delle attività di trattamenti, ai sensi dell'art. 30 del Gdpr, ed infine nell'adozione di misure di sicurezza tecnologiche ed organizzative per proteggere i dati.

Di contro, da un punto di vista formale, il legislatore europeo richiede la precisa individuazione dei ruoli privacy di quei soggetti che orbitano all'interno del Condominio.

Tale ultima questione, in ambito condominiale, si presenta tutt'altro che lineare e di agevole soluzione in virtù di due circostanze: la discussa natura giuridica del Condominio medesimo, ente di gestione con una personalità giuridica "frammentata", non piena sotto il profilo patrimoniale, ma tuttavia capace di contrarre autonomamente tramite il suo rappresentante, destinatario specifico di obblighi di natura fiscale, e il fatto che i soggetti condominiali assumono tendenzialmente tutti posizioni duali.

Difatti, se per un verso i condòmini singolarmente individuati sono qualificabili, senza ombra di dubbio, come interessati, ossia ex art. 4 GDPR "…*le persone fisiche i cui dati personali o particolari risultano trattati da altri",* per altro verso i medesimi soggetti andranno a comporre l'assemblea condominiale, finendo con l'assumere, globalmente considerati, anche la qualifica di titolare del trattamento.

Di talché, emerge la difficoltà di delineare in maniera univoca e definita i ruoli privacy.

A voler seguire le indicazioni del Garante della Privacy, dettate con atto del 18 maggio 2006, il titolare del trattamento nell'ambito condominiale è da individuarsi nel complesso dei condomini organizzati per la gestione della cosa comune (la compagine

condominiale) e, segnatamente l'organo sovrano deputato a determinare gli indirizzi operativi, cioè l'assemblea.

Tuttavia, vi è chi ritiene che il titolare del trattamento possa essere l'amministratore del condominio, in ragione dell'attribuzione allo stesso della responsabilità legale dell'ente di gestione[24], così come, da altra parte, può sostenersi la possibilità di assegnare all'amministratore medesimo contestualmente sia il ruolo di titolare che di responsabile.

A ciò si aggiunga che la nuova normativa prevede la figura del contitolare, nel caso in cui per il medesimo trattamento di dati si indichino contemporaneamente due o più soggetti titolari, che determinano congiuntamente le finalità e gli strumenti del trattamento, e che possono, sulla base di un contratto scritto, da portare a conoscenza degli interessati, ripartire le responsabilità secondo la propria area di competenza.

A ben guardare, però, l'Amministratore di condominio è il soggetto che "naturalmente" viene ad essere chiamato quale Responsabile del trattamento, che opera quindi per conto del titolare del trattamento dei dati (il condominio), e che assume l'obbligo di proteggere e garantire i diritti degli interessati (i condòmini, gli inquilini), riducendo per quanto possibile i rischi di violazione o perdita, anche accidentale, dei propri dati.

La formalizzazione di questo rapporto deve avvenire per il tramite dell'assemblea dei condomini, che all'atto di nomina dell'amministratore dovrà conferire allo stesso la qualifica di responsabile del trattamento, e che in base all'art. 28 comma 9 Gdpr, sarà regolato dal contratto o da altro atto giuridico "*stipulato in forma scritta, anche in formato elettronico*".

L'eventuale strumento giuridico diverso dallo specifico contratto *ad hoc*, idoneo comunque a soddisfare questa prescrizione, ben potrebbe essere costituito da una delibera condominiale o dalla determinazione demandata ad organismi da essa preventivamente individuati, atti a cui l'amministratore, in quanto espressione della volontà condominiale, ex art. 1130 c.c., sarà obbligato ad attenersi.[25]

[24] GIULIANI-MUSCATIELLO, *op. cit.*, Roma, 2019, p.92.

[25] GIULIANI-MUSCATIELLO, *La responsabilità dell'amministratore di condominio*, Roma, 2019, p.88-97.

Il contratto di affidamento, ovvero altro atto giuridico idoneo, impone l'individuazione degli obblighi e, pertanto, sarà necessario procedere alla analitica indicazione dei compiti con la specificazione della durata, della natura e delle finalità del trattamento. Inoltre, sarà opportuno circoscrivere la tipologia dei dati personali da trattare, la precipua individuazione dei limiti di utilizzo dei dati raccolti, gli obblighi e i diritti del titolare del trattamento, così come previsto dall'art. 28 terzo comma del GDPR.

Il responsabile del trattamento, ossia l'amministratore condominiale, laddove non sia stato adottato un altro modello privacy, tratta i dati personali esclusivamente su istruzione documentata del titolare del trattamento, e soltanto previa autorizzazione scritta del titolare, specifica o generale, potrà affidare in tutto o in parte il trattamento dei dati a terzi, essendo prevista la possibilità di nomina del sub-responsabile, pur nel rispetto dell'obbligo di comunicazione al titolare di eventuali modifiche che dovranno da quest'ultimo essere condivise, ovvero conosciute ed approvate.

In ogni caso, laddove l'Amministratore si avvalga di soggetti, suoi dipendenti, che andranno a trattare materialmente i dati personali, gli stessi, ex art. 2 *quaterdecies* del Dlgs 196/2003, così come modificato dalla L. 101/2018, dovranno essere formalmente nominati quali "autorizzati o designati " al trattamento e dovranno essere debitamente istruiti sui compiti da svolgere e circa le precauzioni da adottare per evitare *data beach*, oltre che preparati a gestire eventuali perdite, o mancata disponibilità di dati personali.

In tal senso, il responsabile ex art. 28 par. 3 lettera c del Gdpr, garantisce "…*che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza".*

3. Il trattamento dei dati tra minimizzazione e consenso

Il principio di trasparenza, funzionale alla realizzazione dell'autodeterminazione informativa dell'interessato, prevede che il soggetto, i cui dati si riferiscono, sia edotto delle caratteristiche essenziali del trattamento che lo riguarda, con specificazione dei rischi e delle garanzie previste, al fine di consentirgli l'esercizio dei diritti riconosciuti dal legislatore europeo.

In particolare, come precisato dal considerando 39, devono essere trasparenti per le persone fisiche le modalità con cui sono raccolti ed utilizzati, consultati o altrimenti

trattati i dati personali che li riguardano, nonché la misura in cui i dati stessi sono o saranno trattati.

Da altra angolazione, l'adozione di modalità leali e corrette di gestione del trattamento da parte del titolare presuppone che venga offerta una compiuta ed effettiva comunicazione all'interessato, per cui ai sensi dell'art. 12 del Gdpr, tutte le informazioni dovranno essere fornite *"in forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro"*, eventualmente anche utilizzando immagini o icone.

Il principio, quindi, è declinato nell'ambito degli obblighi del titolare, al quale sono imposti specifici oneri comunicativi, la cui violazione determina l'illiceità del trattamento.

Il risvolto pratico di tale previsione in ambito condominiale, prendendo a prestito le parole del legislatore europeo, è rappresentato dal fatto che l'amministratore, qualora i dati personali siano raccolti presso l'interessato, dovrà confezionare una informativa che tenga conto di tutte le prescrizioni imposte dalla normativa vigente e che, quindi, contenga le informazioni necessarie a garantire un trattamento corretto e trasparente e che, al contempo, sia rispondente alla realtà del trattamento medesimo.

Pertanto, ai fini dell'esecuzione del mandato conferitogli dall'assemblea condominiale, l'amministratore, prima dell'inizio del trattamento, ossia nel momento in cui entra in possesso dei dati personali riferibili ai singoli condòmini, deve mettere a disposizione del soggetto una adeguata, precisa e puntuale informativa.

Il contenuto di tale informativa ha carattere vincolato, e ai sensi dell'art.13 GDPR, deve obbligatoriamente includere taluni elementi tra i quali:

- l'identità e i dati di contatto del titolare del trattamento ed ove applicabile i loro rappresentanti;

- le categorie di dati trattati e finalità del trattamento;

- la base giuridica del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi;

- natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di tale rifiuto;

- se il titolare ha intenzione di utilizzare i dati per una finalità diversa da quella per la quale sono stati raccolti;

- soggetti destinatari (anche per categorie) ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);

- se il titolare ha intenzione di trasferire i dati in paesi extra UE, nel qual caso se esiste o meno una decisione di adeguatezza della Commissione UE (ovvero se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato, per cui il trasferimento non necessita di autorizzazioni specifiche);

- il periodo di conservazione dei dati oppure l'indicazione dei criteri per determinarlo;

- i diritti dell'interessato (diritto di accesso ai dati personali, di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano, di opporsi al trattamento, di revocare il consenso, diritto di presentare reclamo all'autorità di controllo, eventuale diritto alla portabilità)[26].

L'adempimento informativo, in cui ruolo determinante è rivestito dalla indicazione della base giuridica e della finalità di utilizzo dei dati raccolti, obbliga ad una costante ricerca di equilibrio tra minimizzazione e consenso, dovrà essere espletato oltre che nei confronti dei singoli condòmini, anche nei riguardi di quei soggetti di cui l'amministratore si trovi a trattare i dati personali, quali fornitori di servizi e dipendenti del Condominio, nonché per tutti i soggetti che transitano nell'area condominiale e di cui si raccolgono i dati.

Tale documento dovrà essere reso per iscritto o con altri mezzi, anche elettronici, quali la posta elettronica, anche in formato semplificato. Inoltre, è ammessa la possibilità di pubblicare l'informativa sul sito e/o piattaforma condominiale, se esistente, come pure può essere allegata alle comunicazioni e alla corrispondenza, ove ciò si renda necessario al fine di attualizzare ed aggiornare le informazioni privacy già fornite.

[26] BASSOLI, *La nuova privacy gdpr dopo il d.lgs 10 agosto 2018, n.101,* Roma, 2018, p.16-27.

Per quanto concerne la tipologia di dati che possono essere oggetto di trattamento da parte del Condominio, bisognerà innanzitutto richiamare la disciplina prevista nel codice civile, che in generale fa riferimento a tutte quelle informazioni personali e patrimoniali necessarie al soddisfacimento degli obblighi ivi previsti.

In prima approssimazione, quindi, può dirsi che la normativa di settore faccia esplicito rinvio ai dati patrimoniali e personali dei condomini-proprietari, e/o titolari di diritti reali di godimento, ovvero dei condomini-conduttori in ragione della sussistenza di un contratto di locazione, tutti elementi richiesti per la redazione e tenuta dei registri condominiali.

Pertanto, accanto ai dati relativi a consumi collettivi del condominio, potranno essere raccolti i dati anagrafici e gli indirizzi dei partecipanti, elementi la cui reciproca conoscenza, alla luce delle disposizioni contenute nell'art. 66 disp. att. c.c., potrà risultare indispensabile per consentire la regolare convocazione dell'assemblea, nonché per verificare la validità delle deliberazioni dalla stessa adottate, ai fini dell'impugnazione ex art. 1137 c.c. Del pari, possono formare oggetto di trattamento anche le quote millesimali attribuite a ciascuno dei condomini e i dati personali necessari a commisurarle o, comunque, rilevanti per la determinazione di oneri nell'ambito condominiale (art. 68 disp. att. c.c. e art. 1123 c.c.). Le quote millesimali sono dati utili a ricavare il quorum per la regolare costituzione dell'assemblea (quorum costitutivo) e per la validità delle deliberazioni adottate (quorum deliberativo), secondo quanto disposto dall'art. 1136 c.c.

Tali informazioni, riferibili a ciascun partecipante all'assemblea, oltre che al condominio tutto, possono essere trattate esclusivamente per la finalità di gestione ed amministrazione del condominio, così ad esempio, indirizzi e dati anagrafici, saranno utilizzati solo per la convocazione delle assemblee condominiali, ma non potranno essere divulgati per finalità eccedenti.

Tuttavia, le esigenze di trasparenza ed efficienza della gestione del bene comune, che devono coniugarsi con la tutela della riservatezza dei singoli interessati, obbligano comunque il titolare del trattamento a restringere il campo delle informazioni utilizzabili ai soli dati pertinenti e necessari all'attività di gestione ed amministrazione delle parti o dei servizi comuni, riguardanti la compagine condominiale, ovvero ciascun partecipante.

Il principio di minimizzazione, pertanto, opera come in passato, nel senso di perimentrare i dati raccolti, che non dovranno essere più di quelli ritenuti utili a soddisfare le esigenze imposte dalla normativa di settore, adottando, se del caso, modalità che consentono di trattare i dati in forma aggregata, anonimizzata o pseudonimizzata, e limitando la conservazione degli stessi per il tempo strettamente necessario al conseguimento delle finalità del trattamento comunicato all'interessato.

Il trattamento dei dati summenzionati diviene legittimo anche senza il consenso dell'interessato in ragione dell'operatività delle altre condizioni di liceità di cui all'art. 6, innalzate dal Gdpr a rango di prerequisito per il trattamento stesso.

In tal senso, se la legittimità del trattamento dei dati, in ambito condominale, deriva in maniera determinante dall'adempimento di uno specifico obbligo di legge, o in subordine dall'esistenza di un interesse legittimo del Condominio al trattamento, tale da giustificare la compressione del diritto alla riservatezza dell'interessato, tuttavia, le informazioni concernenti, ad esempio, le utenze telefoniche non risultanti da elenchi pubblici potranno essere trattate solo col consenso espresso dell'interessato, nei limiti non eccedenti le finalità di gestione della cosa comune.

Analogo discorso dovrà strutturarsi anche per le informazioni personali, quali gli indirizzi di posta elettronica o eventuali account su social network, che potranno essere trattate solo se espressamente autorizzate e specificamente indicate dall'interessato per il soddisfacimento delle esigenze di reperibilità, contatto o comunicazione in genere, della gestione condominiale. Non potranno essere oggetto di elaborazione quei dati che riguardano le condizioni personali degli interessati, quali la composizione dei rispettivi nuclei familiari, stato civile, abitudini di vita, condizioni patrimoniali, frequenza nella partecipazioni alle attività condominiali[27].

Infine, per quanto concerne i dati che ai sensi dell'art. 9 del GDPR vengono definiti particolari, ossia quelli che *"... rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, ...dati genetici e biometrici intesi a identificare in modo univoco una persona fisica, ...dati relativi alla salute o alla vita sessuale o all'orientamento sessuale",* gli stessi, stante l'esplicito divieto di utilizzo, potranno essere trattati in ambito condominiale solo per effetto dell'espresso consenso dell'interessato.

[27] SAETTA, *Condominio e privacy* in https://protezionedatipersonali.it/condominio-e-privacy.

Tali informazioni particolari, si pensi ad esempio a quelle relative a persone diversamente abili al fine di provvedere all'installazione di un cd. servo-scala per accedere dalle parti comuni alla propria abitazione, così come pure quelle giudiziarie, relative alla qualità di indagato o imputato, possono essere trattate esclusivamente nei casi in cui ciò sia indispensabile ai fini dell'amministrazione del condominio e non per finalità differenti, ma comunque mai senza il consenso dell'interessato.

Laddove la condizione di legittimità del trattamento non sia riconducibile, ad esempio, alla previsione dell'obbligo di legge, ma ricada, invece, in quella riguardante la prestazione del consenso, questo deve essere libero, specifico, informato ed inequivocabile: atto con cui l'interessato manifesta mediante dichiarazione che i dati personali che lo riguardano possono essere oggetto di trattamento.

Egli conserva, in ogni caso, il diritto di revocare il consenso, di chiedere al titolare del trattamento l'accesso ai dati personali, la rettifica o la cancellazione degli stessi, di alcuni dati se non necessari rispetto alla gestione dell'immobile ed all'adempimento degli oneri contrattuali in capo all'amministratore.

Ogni condòmino, inoltre, ha il diritto a vedere corretti i propri dati previa comunicazione all'amministratore di condominio, il quale ha l'obbligo di evadere la richiesta entro un mese. Nelle ipotesi di manifesta infondatezza e ripetitività delle richieste, il titolare dei dati può addebitare un contributo o rifiutarsi di soddisfare la richiesta.

Il mancato rispetto di tali obblighi determina l'illegittimità del trattamento.

In tal senso, deve dirsi illegittimo e conseguentemente sanzionato il comportamento del Condominio, che abbia, ad esempio, effettuato un trattamento di dati mediante un impianto di videosorveglianza omettendo di indicare il titolare del trattamento nei cartelli recanti l´informativa di cui all´art. 13 del Codice, ovvero che abbia proceduto ad una raccolta di dati personali (nome, cognome, estremi del documento di riconoscimento, numero di targa e tipo di autoveicolo) di soggetti estranei al Parco-Condominio i quali chiedevano l´accesso allo stesso, senza che venisse loro resa l´informativa di cui all´art. 13 del Codice.[28]

4. Il Registro di anagrafe condominiale tra diritto di accesso e riservatezza

[28] Garante della Privacy, ordinanza n. 417 del 12 ottobre 2016, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6522175*

La legge n. 220 del 11 dicembre 2012 ha notevolmente ampliato le competenze attribuite all'amministratore, inserendo la previsione dell'obbligo di tenuta di una serie di registri, ipotesi che, in modo particolare per quanto concerne il Registro di Anagrafe Condominiale, impatta sulla normativa relativa alla protezione di dati personali.

Infatti, ai sensi del comma 6 dell'art. 1130 c.c, l'amministratore deve: "…*curare la tenuta del registro di anagrafe condominiale contenente le generalità dei singoli proprietari e dei titolari di diritti reali e di diritti personali di godimento, comprensive del codice fiscale e della residenza o domicilio, i dati catastali di ciascuna unità immobiliare, nonché ogni dato relativo alle condizioni di sicurezza delle parti comuni dell'edificio*".

L'attività prescritta dalla normativa di settore è da considerarsi quale tipica operazione di trattamento dei dati, la cui base giuridica è riconducibile all'adempimento di un obbligo di legge, venendosi, in tal modo, a determinare un collegamento tra la protezione dei dati e la normativa di settore che finisce per evitare il rischio di possibili antinomie all'interno dell'ordinamento.

Il legislatore del 2012, al fine di garantire una maggiore trasparenza attraverso la compilazione costante e aggiornata di un elenco contenente i dati personali e immobiliari dei soggetti che partecipano alla vita condominiale, ha previsto in capo all'amministratore un vero e proprio onere di verifica sull'effettiva appartenenza al Condominio, che implica l'adozione di una serie di comportamenti di gestione e di supervisione volti ad offrire un elevato grado di certezza in ordine alla composizione dell'anagrafe condominiale.

Ed in tal senso, l'amministratore dovrà registrare ogni variazione che riguardi il Condominio, non limitandosi a raccogliere i soli dati dei proprietari delle unità immobiliari, bensì si dovrà attivare al fine ottenere anche quelli dei soggetti titolari di altri diritti reali (usufruttuari) e personali di godimento (conduttori e comodatari). D'altra parte anche gli inquilini, ancorché mediante convocazione da parte dei locatori e seppur limitatamente alle questioni inerenti le spese e le modalità di gestione dei servizi di riscaldamento, hanno il diritto di partecipare all'assemblea e di votare al posto del proprietario.

Infatti, i dati dovranno essere aggiornati stante la previsione di cui al comma 6 dell'art. 1130 c.c p a mente del quale "*Ogni variazione dei dati deve essere comunicata*

all'amministratore in forma scritta entro sessanta giorni. L'amministratore, in caso di inerzia, mancanza o incompletezza delle comunicazioni, richiede con lettera raccomandata le informazioni necessarie alla tenuta del registro di anagrafe. Decorsi trenta giorni, in caso di omessa o incompleta risposta, l'amministratore acquisisce le informazioni necessarie, addebitandone il costo ai responsabili.".

Pertanto, con l'obiettivo di fotografare la composizione della compagine condominiale nei suoi cambiamenti, il Registro di Anagrafe condominiale consente, altresì, di agevolare i rapporti interni, tra comproprietari e tra questi ultimi e l'amministratore, e ottimizzare la gestione delle relazioni esterne con i privati e con le pubbliche autorità, che potrebbe comportare la possibile circolazione di informazioni personali.

L'interpretazione del comma 6 dell'art. 1130 c.c. unitamente all'art. 6 par. 1 lettera c del Regolamento Europeo 675/16 consente di qualificare gli elementi che vanno a comporre il registro di anagrafe condominiale alla stregua del dato personale, trattandosi di *"informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"[29].

Il richiamo alla disciplina sulla tutela dei dati, implica anche relativamente all'obbligo di tenuta del registro dell'anagrafe condominiale, l'operatività del principio di minimizzazione, per cui dovranno essere oggetto di tale trattamento soltanto le informazioni che riguardano ciascun partecipante alla compagine condominiale, individualmente considerato, purché le stesse siano pertinenti e di stretta necessarietà. In definitiva, si tratterà di raccogliere solo quei dati prescritti dalla norma, e non altri, senza che si inseriscano nel Registro di anagrafe condominiale indicazioni ulteriori, né annotazioni e/o commenti di alcun tipo.

Pertanto, in base alla disciplina vigente, così come confermato anche dal Garante, l'amministratore potrà legittimamente *"acquisire le informazioni che consentono di identificare e contattare i singoli partecipanti al condominio, siano essi proprietari, usufruttuari, conduttori o comodatari, chiedendo le generalità comprensive*

[29] Art. 4 par. 1 del GDPR in *http://www.privacy-regulation.eu/it/4.htm.*

di codice fiscale, residenza o domicilio. Può chiedere inoltre i dati catastali: la sezione urbana, il foglio, la particella, il subalterno e il Comune"[30] di ciascuna unità immobiliare, e ogni altro dato relativo alle condizioni di sicurezza delle sole parti comuni dell'edificio, senza che per essi si debba procedere alla richiesta del consenso, stante l'operatività della base giuridica di cui all'art. 6 par. 1 lett. c. del GDPR.

Tale condizione di liceità, individuata nell'obbligo legale, richiede che la misura legislativa alla quale il titolare deve uniformare il proprio comportamento sia chiara, precisa, così come prevedibile deve essere la sua applicazione, in modo da garantire l'effettività del diritto all'autodeterminazione informativa.

Analogo discorso dovrà, quindi, strutturarsi anche per le informazioni personali dei condomini-non proprietari, ossia titolari di diritti reali di godimento, ovvero dei condomini-comodatari o conduttori, quest'ultimi in ragione della sussistenza di un contratto di locazione, per i quali l'amministratore di condominio tratterà i relativi dati in base allo specifico obbligo di legge, individuabile nell'art. 1130, I co., n. 6) c.c. e nella Legge 431/1998, che prescrivono in capo al locatore di dare comunicazione all'Amministratore dell'intervenuta locazione dell'immobile e dei dati del locatario, entro sessanta giorni dalla registrazione del contratto, proprio al fine dell'aggiornamento dell'anagrafe condominiale[31].

Di contro, così come evidenziato con provvedimento del 19 maggio 2000 dal Garante per la Protezione dei dati, solo in presenza del consenso dell'interessato, salva l'eventuale pubblicità già attribuita a tali informazioni grazie alla loro indicazione in elenchi pubblici, potranno essere trattati, in quanto non eccedenti rispetto alla finalità di amministrazione della cosa comune, i dati relativi alle utenze telefoniche intestate ai singoli partecipanti. Il loro utilizzo, infatti, può facilitare, specie in relazione a casi particolari di necessità ed urgenza, ad esempio al fine di prevenire o limitare eventuali danni a parti individuali o comuni dell'immobile, i contatti tra i partecipanti come pure lo svolgimento delle incombenze rimesse all'amministratore del condominio[32].

[30] Garante per la Protezione dei dati, newsletter n. 387 del 23 aprile del 2014 in *https://www.garante-privacy.it/web/guest/home/docweb/-/docweb-display/docweb/3070028*
[31] PALMA, *Condominio e privacy: le nuove linee guida del Garante*, Roma, 2019.
[32]Garante per la Protezione dei dati, provvedimento del 19 maggio 2000 in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/42268*

L'uscita dalla compagine condominiale di un determinato interessato, con l'assolvimento delle obbligazioni a suo carico derivanti dalla relativa gestione, non giustifica più il trattamento dei dati precedentemente acquisiti, i quali, non solo verranno cancellati dal registro dell'anagrafe condominiale, ma non potranno essere più oggetto di alcun lecito trattamento.

Tale disciplina, nel dichiarato intento di rendere effettivo il principio di trasparenza, attraverso la creazione di un "*Condominio di vetro*", di turatiana memoria, in virtù del quale avere una costante ed aggiornata conoscenza dei membri della compagine condominiale, oltre che per consentire la realizzazione di un controllo delle relative attività di gestione, non offre, tuttavia, indicazioni più puntuali circa le modalità di contemperamento con la riservatezza dei dati dei condomini-interessati.

In particolare, resta da risolvere la delicata questione che concerne proprio la tipologia dei dati personali ostensibili, ossia quei dati che l'amministratore può legittimamente comunicare in caso di richiesta di accesso sia da parte dei condomini che di terzi-creditori, senza incorrere in sanzioni.

Per quanto riguarda le richieste provenienti da terzi, creditori del condominio, l'art. 63, 1°comma, disp. Att. c.c. ha previsto che l'Amministratore debba comunicare ai creditori non ancora soddisfatti che lo interpellino i dati dei condòmini morosi, obbligo a cui lo stesso non potrà sottrarsi richiamando il regolamento europeo.

Di contro, i singoli condòmini, senza neppure dover giustificare la propria richiesta, sono titolari *ex lege* del diritto di accedere a tutta la documentazione condominiale, ricomprendendo in tale generica accezione, non soltanto gli atti che riguardano lo stato dei pagamenti degli oneri condominiali e delle eventuali liti pendenti, ma anche tutti i registri previsti dalla disciplina di settore. Possono altresì, accedere alla documentazione relativa al conto corrente condominale, aperto ed utilizzato dall'Amministratore: i condòmini, infatti, sono titolari di una posizione giuridica che consente loro di verificare la destinazione dei propri esborsi e l'operato dell'amministratore mediante l'accesso in forma integrale, per il tramite dell'amministratore, ai relativi estratti

conto bancari e postali. È riconosciuto, quindi, il diritto di ottenere copia di atti o documenti bancari senza alcuna limitazione, neanche nelle forme di un parziale oscuramento, anche se contengono dati personali di terzi[33].

In tale direzione, quindi, deve leggersi l'art. 1130 bis c.c. che dispone che "*i condomini e i titolari di diritti reali o di godimento sulle unità immobiliari possono prendere visione dei documenti giustificativi di spesa in ogni tempo ed estrarne copia a proprie spese*", e prevede, per converso, che l'amministratore del condominio debba mettere a disposizione dei condòmini la documentazione giustificativa. Del resto, il diritto di accesso dei singoli condomini può dirsi speculare al dovere di informare che, in base alla disciplina del mandato con rappresentanza, impone all'amministratore di condominio, ex art. 1712 e 1713 c.c., un obbligo di comunicazione al mandante dell'esecuzione del mandato, oltre che prescrive il dovere di rendere conto del suo operato.

Pertanto, l'effettivo l'esercizio del diritto medesimo prescrive, ai sensi dell'art. 1129 al comma 2 c.c.,che l'amministratore debba comunicare i luoghi dove sono contenuti i registri anagrafe del fabbricato; verbali di assemblea; nomina e revoca dell'amministratore; registro di contabilità, di cui ai numeri 6) e 7) dell'articolo 1130, nonché i giorni e le ore in cui ogni interessato possa prenderne gratuitamente visione ed ottenere, previo rimborso della spesa, copia da lui firmata.

In buona sostanza, così come pure confermato dalla Corte di Cassazione con ordinanza n. 4686 del 28.02.2018, l'accesso ai documenti condominiali da parte dei condòmini può essere messo in atto in qualunque momento sia in sede di approvazione del rendiconto condominiale, sia durante il corso della gestione.

Il libero accesso alla documentazione condominiale, quindi, non può essere precluso, ovvero enormemente compresso da una delibera assembleare, in ragione del fatto che l'unico limite cui è soggetto il potere di vigilanza e controllo di ogni singolo condòmino, di stretta elaborazione giurisprudenziale, è quello per cui il diritto di accesso non può mai risolversi in un intralcio per l'amministrazione ovvero che le richieste di visione o copia dei documenti devono essere conformi con il principio della correttezza di cui all'art.1175 c.c.[34]

[33] Garante della privacy, Newsletter n. 387 del 23 aprile 2014 in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3070028*
[34] Cassazione n. 12579/2017; Cassazione. n. 19799/2014.

Analoga previsione è presente anche all'art.15 del GDPR a mente del quale "*L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:a) le finalità del trattamento;b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo;g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;..... .....4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui".*

A ben guadare, dunque, la normativa di settore come pure quella europea, articolano una disciplina per cui non potranno essere previsti oneri tali da arrecare un pregiudizio grave all'interessato, nel caso di specie al singolo condòmino, i quali renderebbero la relativa delibera assembleare impugnabile per eccesso di potere. Pertanto, i costi addebitabili per le operazioni compiute, che andranno a gravare esclusivamente sui condòmini richiedenti a vantaggio della gestione condominiale non potranno mai consistere in una spesa sproporzionata. [35]

Proprio la finalità che caratterizza il diritto di accesso dei condòmini, ossia l'esercizio di un potere di controllo sull'operato dell'amministratore, unitamente alle modalità con cui lo stesso può essere esercitato, giustifica la relativa estensione a tutti gli atti condominiali.

In tal senso, anche i dati presenti nell'anagrafe condominiale, necessari a soddisfare le esigenze di certezza della composizione della compagine condominiale, oltre a quella particolare funzione rivolta ad agevolare le comunicazioni, dovranno considerarsi trasmissibili agli altri condomini in virtù del principio di solidarietà, come pure ai terzi fornitori in caso di richiesta espressa ai sensi dell'art. 63 disp.att. cod, civ.

[35] Cassazione Civile n. 15159/2001.

Tuttavia, l'applicazione del principio di minimizzazione comporta che ogni altro dato ulteriore rispetto a quelli indicati, quali mail o recapito telefonico, non debba considerarsi necessario a svolgere la funzione riconosciuta al registro e, pertanto, non sia idoneo ad essere in alcun caso trasmesso a terzi soggetti, siano essi condomini o creditori, a meno che non sia intervenuto il previo consenso dell'interessato alla comunicazione del dato che lo riguarda.

In tale prospettiva, occorre segnalare la pronuncia n. 7192 del 09 aprile 2018 con la quale il Tribunale di Roma ha affrontato la questione relativa alla legittimità della comunicazione di taluni dati personali ricompresi nel registro dell'anagrafe condominiale.

In particolare, è stata accolta *«l'impugnazione avverso il deliberato con cui l'assemblea ha espresso la propria contrarietà, cioè ha negato l'autorizzazione, a che l'amministratore rilasci in favore dell'odierno copia dell'elenco dei recapiti dei singoli condomini, tenuto conto che, per principio generale ciascun condomino ha diritto alla consultazione dei documenti inerenti al condominio e che fra questi l'art. 1130, comma 1, n. 6 cod.civ. comprende anche il registro dell'anagrafe condominiale, contenente le generalità dei singoli proprietari, tra cui include espressamente la residenza e domicilio. Va considerato inoltre che tali informazioni appaiono funzionali anche al controllo da parte del condominio in ordine alla regolarità delle convocazioni dell'assemblea ed alla possibilità per gli stessi, in caso di inerzia dell'amministratore, di provvedere di propria iniziativa alla convocazione della riunione»*.

Il Giudice, quindi, nell'accogliere la domanda del condòmino per l'annullamento della delibera assembleare che aveva respinto la richiesta dello stesso proprietario di avere i recapiti degli altri condòmini, ritenendo che detti recapiti fossero da considerarsi dati sensibili, ha specificato che la giustificazione al diniego è da ritenersi *"infondata e pretestuosa non potendosi qualificare il recapito, fornito da un soggetto nell'ambito di un rapporto giuridico, un dato sensibile e per questo non ostensibile, tanto meno nei confronti di chi partecipa a tali rapporti e tanto meno con riferimento ai rapporti che si stabiliscono nell'ambito della comunità condominiale".* In forza di quanto previsto dall'articolo 1129 c.c. viene ribadito il diritto del condòmino alla consultazione ed alla estrazione dell'intera documentazione condominiale.

Inoltre, sempre l'art. 1129 c.c. prevede che i dati relativi alle generalità e ai recapiti dell'amministratore, quelli riguardanti la polizza di assicurazione dell'amministratore per responsabilità civile non sono coperti da riservatezza.

Infine, il contemperamento fra trasparenza e riservatezza deve essere effettuato anche nelle comunicazione realizzata nelle bacheche dei palazzi e/o in altri luoghi aperti al pubblico, in cui non potranno essere apposti avvisi contenenti dati personali che rendano identificabile, seppure indirettamente, un condòmino.[36]

Ed in tal senso, "*l´esposizione, in una bacheca condominiale posta in luogo accessibile anche ad estranei al condominio, dell´ordine del giorno di un´assemblea che riporti anche la situazione debitoria di singoli condomini, viola i principi di pertinenza e non eccedenza nella diffusione dei dati personali. Il condomino interessato, quindi, può agire per ottenere la rimozione dalla bacheca dei dati relativi alla propria morosità*[37].

Analogamente, all'amministratore è preclusa ogni forma di ammonimento dei condòmini relativamente ad esempio alle modalità di parcheggio negli spazi del cortile che avvenga attraverso la bacheca con esposizione di foto delle auto e delle relative targhe, modalità che viola il regolamento.

5. La videosorveglianza condominiale

L'installazione di videocamere di sorveglianza, a tutela di parti di proprietà esclusiva o di proprietà comune è oggi regolata dall'art 1122-ter c.c., introdotto con L. n.220/2012, che ha definitivamente ammesso la possibilità di utilizzare tale sistema di controllo in ambito condominiale.

La disciplina applicabile si distingue a seconda che le telecamere siano installate per fini comuni ovvero privati.

La videosorveglianza condominiale deve compendiare esigenze contrapposte.

In tal senso, la tutela del patrimonio, dei beni e della proprietà condominiale, nonché la tutela dell'integrità fisica delle persone viene a contrapporsi al diritto alla riservatezza, alla difesa della vita privata ed alla protezione dei dati personali.

[36] Garante della privacy, provvedimento del 08.07.2010 in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1741950*
[37] Provvedimento del 12 dicembre 2001 in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/31007*

L'equilibrio tra questi due poli viene ricercato analizzando le condizioni di liceità dell'istallazione degli impianti sia con riferimento alle finalità di protezione della compagine condominiale e sia nel rispetto della riservatezza.

L'installazione di un impianto di video sorveglianza su parti comuni è definita quale innovazione e, deliberata dall'assemblea condominiale con la maggioranza prevista dall'art. 1136 comma 2 c.c., dovrà essere assunta dai proprietari-condomini, a nulla rilevando la posizione dei conduttori che di fatto risulteranno essere gli effettivi abitanti del condominio. Inoltre, affinché la delibera condominiale sia legittima occorrerà, oltre al raggiungimento dei quorum costitutivo e deliberativo, indicare nel verbale assembleare di approvazione, la finalità specifica di tale installazione, e quindi precisare se trattasi della necessità di salvaguardare la sicurezza dei beni condominiali, nonché l'indicazione dell'angolo di visuale delle riprese e registrazioni, che dovrà essere limitato all'area di ingresso condominiale, ovvero alle parti comuni da proteggere.

Infine è obbligatorio fornire idonea informativa dell'installazione medesima.

Affinché il trattamento sia legittimo occorre il consenso dell'interessato, tuttavia così come evidenziato dal Garante con provvedimento del 08.04.2010, *"nel caso di impiego di strumenti di video sorveglianza la possibilità di acquisire il consenso risulta in concreto limitata dalle caratteristiche stesse dei sistemi di rilevazione che rendono pertanto necessario individuare un'idonea alternativa nell'ambito dei requisiti equipollenti al consenso.."*.

In tale prospettiva, in assenza di consenso, la liceità del trattamento è riconducibile all'operatività dell'art 6 lett.f GDPR, ossia il legittimo interesse del titolare che nel caso di specie è la salvaguardia dei beni condominiali e l'incolumità dei condomini.

Il rispetto della disciplina in punto di protezione dei dati continua a prevedere la segnalazione della telecamera con appositi cartelli in modo da informare gli interessati che stanno per accedere alla zona coperta dal raggio di azione dell'impianto; la conservazione delle videoregistrazioni per un periodo limitato di tempo che non può tendenzialmente superare le 24/48 ore, la necessaria istanza al garante per la conservazione dei dati per tempi superiori alla settimana, la protezione dei dati raccolti con

idonee misure di sicurezza che ne consentano l'accesso alle persone autorizzate (il titolare e il responsabile del trattamento, ovvero ove previsto la società di vigilanza in qualità di sub-responsabile[38].

6. Conclusioni

La normativa sulla tutela dei dati personali ci ha mostrato come una maggiore trasparenza dell'organizzazione e dell'azione degli Enti di Gestione che trattano tali dati abbia innumerevoli vantaggi. Infatti, porre l'attenzione sulla trasparenza, elevandola a principio fondante del nuovo Regolamento europeo, permette di garantire una più estesa visibilità, conoscibilità e comprensibilità delle modalità operative e degli assetti organizzativi dell'ente di gestione che rappresenta un indispensabile presupposto al corretto funzionamento del rapporto giuridico che lega ad esempio il Condominio e i singoli condomini.

Tuttavia, considerare la trasparenza principio generale ed essenziale di ogni trattamento dei dati personali, indipendentemente dal rapporto che può sussistere tra il titolare e gli interessati, e collocarla all'interno di un sistema in cui convive necessariamente con altri diritti fondamentali, se per un verso determina il venir meno di quella visione antagonista che la vedeva contrapposta al diritto alla privacy, dall'altro obbliga l'amministratore di condominio ad uno sforzo continuo rivolto alla costante ricerca di un equilibrio tra trasparenza - diritto di accesso dei condòmini e riservatezza, relativamente ai dati personali oggetto di trattamento in ambito condominiale.

In questa nuova visione, che intreccia liceità, correttezza e trasparenza con *accountabiliy, privacy by design e by default,* che fa convivere le adeguate misure di sicurezza con l'autodeterminazione informativa, l'attività dell'Amministratore, così come quella degli altri soggetti che occupano un ruolo privacy all'interno del Condominio, ciascuno secondo le proprie competenze e responsabilità, dovrà modularsi nella direzione della protezione dei dati personali, al fine di consentire l'affermazione e la diffusione di una nuova cultura della privacy, che prescrive innanzitutto il diritto dell'interessato al controllo dei propri dati personali, sia nella fase genetica del rapporto, strettamente legata alla finalità del trattamento, che nelle successive vicende circolatorie.

[38] GAMBINI, *Videosorveglianza su parti comuni e Regolamento privacy*, in Archivio della locazioni del condominio e dell'immobile, 2019, 1, p. 22-26.

IL CONTROLLO A DISTANZA MEDIANTE SOCIAL NETWORK TRA POSSIBILITA' TECNICHE E LIMITI LEGALI.

di Sergio Giuda

SOMMARIO. 1. Introduzione. - 2. Le reti sociali come fenomeni complessi. - 3. I riferimenti normativi. – 4. Modalità operative, *best practice* e indicazioni giurisprudenziali. – 5. Considerazioni finali.

Nowadays, privacy is almost a chimera and even on the job it finds ever smaller spaces. There is a thin line that separates legitimate employer behaviors from those that are not and that go to harm the privacy of workers, but employers already have the right to control their employees in order to identify illegal behavior. In what limits? Everything concerning remote control, through video surveillance tools such as cameras but also through computer devices such as PCs, smartphones and tablets, has been reformed by the Jobs Act, loosening the nodes but maintaining strong privacy restrictions. Indeed, numerous ordinances have deemed the dismissal based on improper use of social networks legitimate, such as posting photographs taken during working hours accompanied by offensive comments against the company. Basically, the concept behind the judges' decision is that, when you decide to publish certain information and photos on your profile, you automatically accept the risk that these may be seen by third parties and then used in court.

1. Introduzione.

Come noto, nella vita di tutti i giorni la privacy è ormai quasi una chimera, ma anche sul lavoro gli spazi di cui dispone sono sempre più ridotti. Nonostante a volte possa apparire sottile la linea che separa le condotte legittime da quelle che non lo sono, i datori di lavoro hanno la facoltà di controllare i propri dipendenti al fine di individuare comportamenti illeciti. Devono però rispettare alcuni limiti per non andare a ledere la privacy dei lavoratori,.

Tutto ciò che riguarda il controllo a distanza, tramite strumenti di videosorveglianza (ad es. telecamere) ma anche tramite dispositivi informatici quali pc, smartphone e tablet, è stato riformato dal Jobs Act, allentando i nodi ma mantenendo saldi i vincoli di privacy.

Con riferimento specifico ai social network, le verifiche dei datori di lavoro in molti casi partono già dalle fasi del colloquio, andando a verificare i profili sui canali social e proseguono nel corso del rapporto di lavoro. Tale comportamento viene ritenuto lecito da parte del Garante Privacy, anche se alcuni dati vengono reperiti sui social network ricorrendo alla rete di amici comuni piuttosto che inviando richiesta di contatto diretta, e anche se il datore non ha preavvisato il dipendente.

D'altro canto, numerose ordinanze hanno ritenuto legittimo il licenziamento basato su un uso improprio dei social network, come postare fotografie scattate durante l'orario di lavoro accompagnate da commenti offensivi nei confronti dell'azienda. Il concetto alla base della decisione dei giudici è che, nel momento in cui si decide di pubblicare determinate informazioni e foto sul proprio profilo, si accetta automaticamente il rischio che queste possano essere viste da soggetti terzi e quindi utilizzate in tribunale. In nessun caso, però, possono giustificare un licenziamento le informazioni, reperite o meno su Internet, riguardanti dati sensibili come l'orientamento o la vita sessuale di un dipendente, pena la nullità del licenziamento per motivi discriminatori.

2. Le reti sociali come fenomeni complessi

«*Il tema dei "social" è tipicamente multidisciplinare: interessa comunicazione, sociologia, psicologia, medicina e diritto e inoltre alimenta cronaca e giurisprudenza*».[39]

I Social network si identificano, comunemente, in servizi informatici on-line che permettono la realizzazione di reti sociali virtuali. Trattasi di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro.

Generalmente i Social network prevedono una registrazione mediante la creazione di un profilo personale protetto da password e la possibilità di effettuare ricerche nel database della struttura informatica per localizzare altri utenti e organizzarli in gruppi e liste di contatti.

[39] Cfr. D. IODICE, R. COLOMBANI, *Social network e responsabilità disciplinari: le possibili tutele individuali*, in bollettino ADAPT del 17 luglio 2018, n. 27, 1.

Le informazioni condivise variano da servizio a servizio e possono includere dati personali, sensibili (credo religioso, opinioni politiche, inclinazioni sessuali ecc.) e professionali. Sui Social network gli utenti non sono solo fruitori, ma anche creatori di contenuti.

«La rete sociale diventa un ipertesto interattivo tramite cui diffondere pensieri, idee, link e contenuti multimediali».[40]

Un social network è definito come un gruppo connesso di singoli agenti che prendono decisioni di produzione e consumo in base alle azioni (segnali) di altri agenti sul social network; una definizione che dà il primato alle azioni comunicative piuttosto che alla sola connettività. Social qui significa la capacità di un agente di connettersi e interpretare le informazioni generate da altri agenti e di comunicare a loro volta; e rete significa che si tratta di connessioni specifiche (spesso tecnologicamente abilitate) e non di un gruppo aggregato astratto come una nazione, un popolo o simili.[41]

I social media sono una raccolta di tecnologie e applicazioni che consentono alle persone di comunicare, scambiare informazioni e condividere artefatti digitali (ad es. foto e video) spesso nel contesto di gruppi più grandi, comunità o reti. I sistemi di social media sono molto diversi e includono wiki, micro e normali blog, social network online per uso personale e uso professionale, mondi virtuali e online piattaforme comunitarie (Kaplan & Haenlein, 2010).[42]

Una delle conseguenze impreviste più significative dei sistemi di social media per le relazioni professionali è la confusione dei confini tra i contesti sociali. Famiglia, amici e colleghi sono ruoli che spesso esistono in gran parte all'interno di sfere sociali separate. Quando possibile, le persone gestiscono le loro relazioni con amici, famiglia e colleghi di lavoro in modo che gli individui delle diverse sfere non interagiranno o saranno consapevoli di ciascuno altro.

[40] Cfr. D.M. TESTA, *Il controllo a distanza dei lavoratori ed i Social network*, in Jei - Jus e Internet, 23 Febbraio 2017, 1-2.
[41] Cfr. J.D. POTTS, S.D. CUNNINGHAM, J. HARTLEY & P. ORMEROD, *Social network markets : a new definition of the creative industries.* Journal of Cultural Economics, (2008) 32(3), pp. 166-185, 7.
[42] Cfr. B. BUTLER, S. MATOOK, *Social media and relationships*. In: R. MANSEL (ed.) The International Encyclopedia of Digital Communication and Society, First Edition © 2015 John Wiley & Sons, Inc, 1.

Tuttavia, i sistemi di social media, come Twitter o Facebook, hanno l'effetto di riunire queste relazioni (e individui): di conseguenza, sui siti di social network, i confini tra relazioni private e professionali degli individui sono sfocati.[43]

Osserviamo con preoccupazione la recente, progressiva e generale implementazione "social" delle piattaforme informative aziendali. In questi ultimi anni, infatti, moltissime imprese ("digitali" o no) stanno praticando un uso non estemporaneo, ma "organico" dei social.

Le imprese colgono: nel fenomeno "social", nuove opportunità di business; nei propri dipendenti, inediti veicoli di comunicazione commerciale, arrivando ad "incentivare" emotivamente gli stessi ad intraprendere azioni di promozione e proposizione del brand che essi rappresentano. I *social network* (e con essi i lavoratori di ciascuna azienda, sempre più "testimonial" del brand) appaiono insomma pienamente innestati nelle politiche commerciali aziendali.

Cosa ne deriva? Senza dubbio, una crescente pervasività organizzativa, che consente all'impresa di espandere la propria influenza ben oltre gli spazi e i tempi del lavoro "contrattualizzato" (che è oggetto di specifiche tutele giuridiche individuali).[44]

Le motivazioni che inducono le aziende a ricorrervi possono essere varie[45], ma i casi sono soprattutto rivolti a tutelare il patrimonio aziendale in senso ampio, vale a dire tutti gli asset, materiali ed immateriali.

E così «*i Social network, nell'inarrestabile ascesa che li ha visti coinvolti, sono stati in grado di travalicare le porte delle fabbriche, degli uffici e, più in generale, dei luoghi di lavoro. Il web 2.0, grazie alle sue numerose funzionalità, è divenuto una delle numerose tecniche di controllo a distanza sul comportamento del lavoratore-utente*».[46]

3. I riferimenti normativi

[43] Cfr. B. BUTLER, S. MATOOK, *Social media and relationships*. In: MANSEL R. (ed.) The International Encyclopedia of Digital Communication and Society, First Edition © 2015 John Wiley & Sons, cit., 6.
[44] Cfr. D. IODICE, R. COLOMBANI, *Social network e responsabilità disciplinari: le possibili tutele individuali*, in bollettino ADAPT del 17 luglio 2018, n. 27, cit., 1-2.
[45] Si veda per tutti GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Lavoro: le linee guida per posta elettronica e internet*, Del. n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 [doc. web n. 1387522].
[46] Cfr. A. INGRAO, *Il controllo a distanza effettuato mediante Social network*, in LLI, Vol. 2, No. 1, 2016, ISSN: 2421-2695, 105.

Le fonti normative (sia di hard che di soft law[47]) applicabili sono le seguenti:

in ambito «privacy»:

- Provvedimenti vari del Garante per la Protezione dei Dati Personali, sia antecedenti che susseguenti il GDPR[48].
- Regolamento Europeo 2016/679/UE, GDPR[49].
- Parere Gruppo di Lavoro Art.29 (WP29, ora EDPB, European Data Protection Board o Comitato europeo per la protezione dei dati) 2/2017 dell'8 Giugno 2017 sul trattamento dei dati dei lavoratori nei luoghi di lavoro – WP 249[50].

Come accennato, molti Provvedimenti del Garante si basano sul Codice Privacy del 2003 (D.Lgs. 196/2003)[51] e quindi nei testi via via vigenti ma precedenti al GDPR stesso, nei confronti del quale il Codice Privacy è stato poi «armonizzato» con il D.Lgs 101/2018[52].

Per la disciplina giuslavoristica: l'architrave è la normativa sui controlli a distanza dei lavoratori, contenuta nell'art. 4 L. 300/1970[53], di seguito anche «*Statuto dei Lavoratori*», come modificato dal cd. «*Jobs Act*» contenuto nel D. Lgs. 14 settembre 2015, n. 151[54].

---

[47] Sull'ampio dibattito cito ad es. «il fenomeno della soft law, nella sua estrema varietà, non deve essere analizzato nella limitata prospettiva del farsi del diritto, quanto, piuttosto, nel più ampio orizzonte del c.d. regulatory process: ossia, della dinamica che abbraccia la produzione del diritto – nei diversi livelli, centri e modi a ciò deputati –, la sua attuazione (anche attraverso la regolazione) e applicazione in chiave di effettività (meccanismi di enforcement)» in BOSCHETTI B., *Soft law e normatività: un'analisi comparata*, in *Rivista della Regolazione dei mercati, Fascicolo* 2| 2016, 37.

[48] Regolamento del Parlamento europeo e del Consiglio 2016/679/UE, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in Gazzetta ufficiale dell'Unione europea del 4 maggio 2016.

[49] Reg. CE 679/2016, *cit*..

[50] ARTICLE 29 DATA PROTECTION WORKING PARTY, *WP249, Opinion 2/2017 on data processing at work, Adopted on* 8 June 2017.

[51] Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali. (GU Serie Generale n.174 del 29-07-2003-Suppl.Ordinario n. 123).

[52] Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). GU Serie Generale n.205 del 4 settembre 2018.

[53] Legge 20 maggio 1970, n. 300, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale, nei luoghi di lavoro e norme sul collocamento. (GU Serie Generale n.131 del 27-05-1970), cd. Statuto dei lavoratori.

[54] Decreto Legislativo 14 settembre 2015, n. 151 Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183. (15G00164) (GU Serie Generale n.221 del 23-09-2015-Suppl. Ordinario n. 53).

Una novità fondamentale sta nel fatto che ora è proprio l'art. 4 a richiamare il rispetto del Codice Privacy come condizione di utilizzabilità dei dati.

Iniziando allora dalla disciplina lavoristica, il «vecchio» art. 4 dello Statuto dei Lavoratori vietava come noto l'uso degli impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori: «Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.»

C'era un divieto generale di controllo a distanza della prestazione lavorativa e l'eccezione del secondo comma (cd. «*controllo preterintenzionale*» non riguardava il controllo della prestazione ma l'installazione di «*impianti*» e «*apparecchiature*». Da qui la discussa categoria dei «*controlli difensivi*»[55].

L'orientamento consolidato della giurisprudenza di Cassazione, confermato nel 2018[56], è dunque nel senso di ritenere ammissibile e non assoggettabile alle garanzie procedurali di cui all'articolo 4 dello Statuto dei lavoratori il controllo difensivo occulto finalizzato all'accertamento di comportamenti illeciti non riguardanti l'esatto adempimento dell'obbligazione lavorativa ed effettuato *ex post*, «ovvero dopo l'attuazione del comportamento addebitato al dipendente, quando siano emersi elementi di fatto tali da raccomandare l'avvio di un' indagine retrospettiva»[57].

[55] Cfr. ad.es .«*Ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n.300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate*», Cassazione civile, sez. lavoro, sentenza 03/04/2002 n° 4746, in Altalex (online).

[56] Vedasi Cassazione civile, sez. Lavoro, Ordinanza 28/05/2018 n° 13266 in Altalex (online).

[57] Cfr. anche «*I controlli difensivi "occulti" sono tendenzialmente ammissibili in quanto diretti all'accertamento di comportamenti illeciti diversi dal mero inadempimento della prestazione lavorativa restando comunque necessario che le attività di accertamento si esplichino con modalità che contemperino l'interesse del datore al controllo e alla difesa dell'organizzazione con il rispetto delle garanzie di libertà e dignità dei dipendenti, ed in ogni caso rispettino i canoni generali della correttezza e buona fede contrattuale*», Cassazione civile, sez. lavoro, sentenza 27/05/2015 n° 10955, in Altalex (online).

Analogamente in una sentenza della Corte di Cassazione del 2015[58] che si è occupata di un episodio di licenziamento correlato a controlli effettuati via GPS: al lavoratore era stato contestato di essersi allontanato, con l'autovettura della società, dai luoghi dove doveva svolgere il proprio lavoro, e ciò era testimoniato dal «tracciato» correlato al sistema GPS che era stato posizionato sulla vettura. Secondo la Corte non c'è stata violazione della vecchia formulazione dell'articolo 4 dello Statuto dei Lavoratori in quanto simili azioni di controllo sono state ravvisate come rientranti nei «controlli difensivi» volti a tutelare il patrimonio aziendale e a rilevare violazioni specifiche e comportamenti estranei alla normale attività lavorativa, nonché illeciti.

Una delle deleghe del cd. Jobs Act riguardava la «revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore» (art. 1, comma 7, lett. f, legge delega n.183/2014). Conseguentemente, l'articolo 4 dello Statuto dei Lavoratori è stato modificato nella direzione indicata[59].

Nel nuovo articolo 4**:**

- **s**parisce il divieto generale di controllo a distanza della prestazione lavorativa; tuttavia, gli strumenti installati esclusivamente a fini di controllo e la sorveglianza esasperati erano e rimangono illeciti per contrasto con norme costituzionali che prescindono dall'art. 4[60];
- gli impianti da cui derivi anche la possibilità di controllare a distanza la prestazione del dipendente possono essere impiegati esclusivamente per:

[58] Cassazione civile, sez. lavoro, sentenza 12/10/2015 n° 20440, in Altalex (online).
[59] E ora recita, al comma 1: «Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, dalla sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi».
[60] Cfr. "*Non a caso, la Relazione Ministeriale al disegno di legge dello Statuto dei lavoratori già ammoniva che la sorveglianza dovesse essere "mantenuta in una dimensione umana e cioè non esasperata dall'uso delle tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*", in C. CAFIERO**,** *La tutela della privacy del lavoratore*, in *Diritto24.ilsole24ore.com*, 8 ottobre 2018.

√ esigenze organizzative e produttive;

√ sicurezza del lavoro;

√ tutela del patrimonio aziendale;

- gli impianti possono essere installati:

√ previo accordo con RSU/RSA o sindacati nazionali (in caso di più unità produttive in diverse province/regioni).

√ In mancanza di accordo è necessaria l'autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o della sede centrale di tale Ispettorato (nel caso di imprese multi-localizzate).

Al comma 2[61] c'è un'eccezione alla regola generale, relativa a strumenti in continua evoluzione, quali pc portatili, *ipad*, *smartphone*, rilevazione presenze attraverso dati biometrici, tecnologie indossabili, social network: l'accordo sindacale o l'autorizzazione amministrativa di cui al comma 1 non servono.

Tuttavia, il Ministero del Lavoro ha stabilito che nel momento in cui lo strumento viene modificato (ad esempio, con l'aggiunta di software di localizzazione), non si considera più rientrante nella categoria[62].

Il fondamentale comma 3 recita «Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196» (Codice Privacy), come accennavo.

I nuovi obblighi si applicano a ogni trattamento effettuato dal datore di lavoro sulla base dei controlli, sicché:

- senza policy e privacy il trattamento è illegittimo, come le sue conseguenze.
- Lo strumento di lavoro è inteso in senso oggettivo e in relazione diretta con la prestazione. Quindi non esiste una definizione univoca di strumento di lavoro, ma la definizione dipende dall'attività del dipendente, cioè ai fini dell'art. 4 è lo strumento attraverso cui il dipendente rende la prestazione.

[61] «La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze».
[62] Si veda MINISTERO DEL LAVORO, *Controlli a distanza, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy* - Comunicato stampa 18 giugno 2015, in *https://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx.*

- Esorbita dai confini della norma l'aggiunta sullo strumento stesso di componenti (hardware, software) che siano estranei alla prestazione e indirizzati (esclusivamente) al controllo.

  Ho già sottolineato che una novità fondamentale sta nel fatto che è proprio l'art. 4 a richiamare il rispetto del Codice Privacy come condizione di utilizzabilità dei dati.

  Concetto che si ritrova ribadito anche dal Garante per la protezione dei dati personali, quando afferma «*Principi che restano validi anche dopo la riforma dei controlli datoriali operata dal Jobs Act e anche rispetto agli strumenti di lavoro che, pur sottratti alla procedura concertativa, restano comunque soggetti alla disciplina del Codice privacy. E, in particolare, i principi di necessità, finalità, legittimità e correttezza, proporzionalità e non eccedenza del trattamento, nonché l'obbligo di previa informativa del lavoratore e al divieto di profilazione, ribaditi proprio dalla Corte europea dei diritti umani, con la sentenza di ieri*» (CEDU - Sez. IV, 12 gennaio 2016)[63].

  E già nel Provvedimento del 1° marzo 2007, Lavoro: le linee guida del Garante per posta elettronica e internet (cit.), l'Autorità confermava che "le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà. (..) Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l´esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (*artt. 2 e 41,secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l´art. 2, comma 5, Codice dell´amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell´interessato*). Non a caso, nell'organizzare l´attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d´uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe

[63] Cfr. A. SORO, *I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail. Intervento del Presidente del Garante per la protezione dei dati personali* ("L´Huffington Post", 13 gennaio 2016).

di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.[64]

Con il parere n. 2 dell'8 giugno 2017 (*Opinion 2/2017 on data processing at work*), il WP29 (ora "Garante Europeo") ha adeguato all'evoluzione degli strumenti tecnologici il contenuto delle sue precedenti pubblicazioni *Opinion 8/2001 on the processing of personal data in the employment context* e *2002 Working Document on the surveillance of electronic communications in the workplace.*

Ma soprattutto il provvedimento è stato emanato anche per la *compliance* all'applicazione del Regolamento (UE) 2016/679 verso il trattamento dei dati dei lavoratori da parte dei datori di lavoro, rilevabile nel bilanciamento dei diversi interessi in gioco.

Il diritto del lavoratore alla protezione dei propri dati personali in ambito lavorativo, infatti, deve essere bilanciato con i legittimi interessi di natura aziendale perseguiti dal datore di lavoro ("[…] *a new assessment is required concerning the balance between the legitimate interest of the employer to protect its business and the reasonable expectation of privacy of the data subjects: the employees*).

L'EPDB richiama il comma 1 dell'articolo 88 del GDPR, ai sensi del quale è rimessa agli Stati Membri la possibilità di adottare atti normativi specifici volti ad "*assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro*", in particolare per le seguenti finalità:

- assunzione;
- esecuzione del contratto di lavoro;
- gestione, pianificazione e organizzazione del lavoro;
- parità e diversità sul posto di lavoro;
- salute e sicurezza sul lavoro;
- protezione della proprietà del datore di lavoro o del cliente;
- esercizio e godimento, individuale e collettivo dei diritti e dei vantaggi connessi al lavoro;

[64] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Lavoro: le linee guida per posta elettronica e internet*, Del. n. 13 del 1° marzo 2007, Gazzetta Ufficiale n. 58 del 10 marzo 2007 [doc. web n. 1387522], cit., 2.

- cessazione del rapporto di lavoro.

Il comma 2 del medesimo articolo stabilisce l'orientamento dei suddetti atti normativi, il quale deve mirare alla salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, con particolare riferimento: *(i)* alla trasparenza del trattamento, *(ii)* al trasferimento dei dati personali nell'ambito di attività economiche svolte in comune da gruppi imprenditoriali e di imprese e *(iii)* ai sistemi di monitoraggio sul posto di lavoro.

Tra gli scenari trattati, spicca la possibilità per i datori di lavoro di effettuare un controllo dei profili pubblici dei social network dei candidati, ai fini della selezione per determinate posizioni lavorative.

Qualora, infatti, i candidati/interessati siano titolari di profili social e abbiano scelto di mantenere pubbliche le informazioni e i dati personali in essi contenuti, il datore di lavoro in fase di *recruitment* potrà legittimamente effettuare un controllo sui citati profili, al fine di valutare l'idoneità del candidato rispetto alle mansioni proprie della posizione aperta.

Il trattamento e la raccolta dei dati, in ogni caso, deve essere strettamente connessa alla finalità propria che la legittima: la valutazione delle caratteristiche lavorative e delle qualifiche del candidato in base all'offerta di lavoro. Pertanto, non è consentito al datore di trattare e utilizzare tali dati per altre finalità che non siano in linea con la procedura di selezione dei candidati e la verifica dei requisiti lavorativi richiesti per la prestazione lavorativa.

Essendo perseguito in tal senso un legittimo interesse del datore di lavoro, non è necessario raccogliere il preventivo consenso al trattamento da parte del candidato.

Per contro, il Garante Europeo richiede l'attività informativa del trattamento in oggetto da parte del datore di lavoro in una fase precedente al trattamento stesso, proponendo tra le soluzioni l'inserimento già nell'annuncio di lavoro dell'informativa relativa alla verifica dei profili social pubblici dei candidati.

Il datore di lavoro che ha trattato e raccolto i dati personali del candidato per le finalità sopra esposte, dovrà però provvedere alla tempestiva cancellazione dei medesimi nel momento in cui la posizione lavorativa non venga ricoperta dal candidato stesso.

Anzi, le novità introdotte dal Regolamento (UE) 2016/679, specie quelle in tema di privacy by design[65] e privacy by default[66], rafforzano sensibilmente le tutele già indicate nei provvedimenti di soft law fin qui richiamati.

In particolare, il principio di privacy by design nell'ottica del rapporto tra datore di lavoro e lavoratore, che in questa sede interessa, impone che i sistemi siano progettati in maniera tale da operare, anche in via automatica, una selezione delle informazioni raccolte, evitando l'utilizzo e la diffusione di dati non rilevanti ai fini della gestione e organizzazione del rapporto di lavoro.

Va considerato che, attraverso il controllo dei social network, il datore di lavoro (che è titolare del trattamento, ai sensi dell'art. 24 GDPR) effettua trattamenti di dati personali dei lavoratori/interessati al trattamento, anche appartenenti a categorie particolari di dati personali (art. 9 del GDPR).

Già nel 2014 il Garante per la protezione dei dati personali[67], giudicando lecite le finalità perseguite e rispondenti ad esigenze organizzative e produttive nonché di sicurezza del lavoro, ritenne il trattamento ammissibile in quanto conforme ai principi di

---

[65] Cfr. «*Nel contesto internazionale è presente la descrizione ben strutturata della Privacy by Design, frutto della elaborazione di Ann Cavoukian (che, quale Information and Privacy Commissioner of Ontario, Canada, fu tra i promotori della risoluzione adottata nel 2010). Secondo questa impostazione, l'utente è considerato il centro del sistema privacy (per definizione, quindi, è "user centric"). Qualsiasi progetto (sia strutturale sia concettuale) va realizzato considerando dalla progettazione (appunto by design) la riservatezza e la protezione dei dati personali. La PbD comprende una trilogia di applicazioni (1. sistemi IT; 2. pratiche commerciali corrette; 3. progettazione strutturale e infrastrutture di rete) e vengono individuati 7 principi definiti fondazionali che esprimono pienamente l'intero senso di questa prospettiva (1. Proattivo non reattivo – prevenire non correggere; 2. Privacy come impostazione di default; 3. Privacy incorporata nella progettazione; 4. Massima funzionalità − Valore positivo, non valore zero; 5. Sicurezza fino alla fine − Piena protezione del ciclo vitale; 6. Visibilità e trasparenza − Mantenere la trasparenza; 7. Rispetto per la privacy dell'utente − Centralità dell'utente)*» in FABIANO N., *Privacy by Design: l'approccio corretto alla protezione dei dati personali*, in *Diritto24.ilsole24ore.com*, 20 aprile 2015.

[66] Cfr. "*L'impostazione predefinita determina come funziona il sistema se non viene modificato nulla. Pertanto, non è solo il punto di partenza del modo in cui viene utilizzato il sistema, ma poiché molti utenti non cambieranno mai l'impostazione predefinita, ne governerà l'utilizzo in larga misura [Kesan, 2006]. Questo vale anche per la privacy e la protezione dei dati. Quando Cavoukian ha sviluppato i principi fondamentali per la privacy in base alla progettazione, ha dedicato un principio alla "Privacy come impostazione predefinita: se un individuo non fa nulla, la sua privacy rimane intatta. Non è richiesta alcuna azione da parte dell'individuo per proteggere la propria privacy: per impostazione predefinita è integrata nel sistema*."[CAVOUKIAN, 2011]. Il Garante europeo della protezione dei dati ha elaborato il principio predefinito nel parere sul Pacchetto di riforma della protezione dei dati: "L'idea alla base del principio è che le funzionalità di violazione della privacy di un determinato prodotto o servizio sono inizialmente limitate a quanto è necessario per il semplice utilizzo di esso"[EDPS, 2012]» in ENISA (EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY), *Recommendations on shaping technology according to GDPR provisions Exploring the notion of data protection by default*, December 2018, 11.

[67] Cfr. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone. Verifica preliminare richiesta*

necessità, pertinenza e non eccedenza, precisando, tuttavia, alcune limitazioni: a) adottare misure e accorgimenti tecnici ispirati ad una logica di privacy by design, idonei a garantire che le informazioni presenti sul dispositivo mobile, visibili e utilizzabili dall'applicazione installata fossero riferibili soltanto ai dati potenzialmente lesivi dei propri asset, nonché a impedire l'eventuale trattamento di dati ultronei (quali quelli relativi al traffico telefonico, agli sms, alla posta elettronica); b) consentire l'eventuale trattamento dei dati in tempo reale solo in presenza di specifiche esigenze (ad esempio, legate al verificarsi di situazioni di emergenza e/o di pericolo per il dipendente), individuate all'interno di appositi protocolli; c) consentire l'accesso ai dati trattati ai soli incaricati della società che, in ragione delle mansioni svolte o degli incarichi affidati, potessero prenderne legittimamente conoscenza.

E il WP29 «ribadisce la posizione e le conclusioni del parere 8/2001 e del documento di lavoro del WP55, vale a dire che durante l'elaborazione dei dati personali dei dipendenti:

- i datori di lavoro devono sempre tenere presente i principi fondamentali di protezione dei dati, indipendentemente dalla tecnologia utilizzata;
- i contenuti delle comunicazioni elettroniche effettuate da locali commerciali godono delle stesse protezioni dei diritti fondamentali delle comunicazioni analogiche;
- è improbabile che il consenso costituisca una base giuridica per l'elaborazione dei dati sul lavoro, a meno che i dipendenti non possano rifiutare senza conseguenze negative;[68]
- l'esecuzione di un contratto e gli interessi legittimi possono talvolta essere invocati, a condizione che l'elaborazione sia strettamente necessaria per uno scopo legittimo e sia conforme ai principi di proporzionalità e sussidiarietà;
- i dipendenti devono ricevere informazioni efficaci sul monitoraggio che ha luogo» [69].

---

da Ericsson Telecomunicazioni S.p.a. - *Provvedimento* n. 401 dell´11 settembre 2014 [doc. web n. 3474069].

[68] In realtà vari studi hanno rivelato «i limiti del consenso preventivo, sia perché reso inconsapevolmente sia perché – anche quando è reso consapevolmente – non si traduce in un effettivo impedimento alla dannosità del trattamento per la persona dell'utente, dannosità che continua a potersi verificare. Al contrario, la prestazione del consenso potrebbe avere un effetto distorsivo perché esso viene prestato senza che l'utente abbia cognizione degli strumenti di tutela ex post ed anzi sulla base della convinzione che la sola concessione del consenso elimini a priori la possibilità stessa di una lesione» in L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, Politica del diritto, 2017, 2, 350.

[69] ARTICLE 29 DATA PROTECTION WORKING PARTY, *WP249, Opinion 2/2017 on data processing at work, Adopted on* 8 June 2017, cit., 1.

In particolare il gruppo di lavoro mira ad evidenziare il «bilanciamento tra il legittimo interesse dei datori di lavoro e le ragionevoli aspettative di privacy dei dipendenti, ivi incluso il diritto alla loro riservatezza; successivamente vengono individuate le basi giuridiche di tale trattamento, che possono ravvisarsi, alternativamente:

(i) nell'esecuzione di obblighi derivanti da un contratto di lavoro, ove presente (es.: finalità retributive, ai sensi dell'art. 6.1, lett. b) GDPR);

(ii) nell'adempimento di obbligazioni previste dalla legge (es.: calcolo della ritenuta d'imposta, ex art. 6.1, lett. c) GDPR);

(iii) nell'interesse legittimo del datore di lavoro (es.: prevenzione della perdita di materiali aziendali e/o miglioramento della produttività dei lavoratori, ex art. 6.1, lett. f) GDPR).

Viene ribadita l'esclusione dalle basi giuridiche del mero consenso dei lavoratori in quanto, a causa del rapporto di dipendenza nei confronti del datore di lavoro, lo stesso consenso non potrebbe ritenersi liberamente prestato né revocabile. Quindi, nel trattare dati dei dipendenti, il datore di lavoro deve tenere ben presenti i diritti fondamentali dei lavoratori, e individuare correttamente la base giuridica di tale trattamento.[70]

Per quanto riguarda in particolare l'interesse legittimo del datore di lavoro, poi, quest'ultimo deve

- valutare preventivamente se il trattamento da porre in essere sia necessario e proporzionato per il perseguimento di una finalità legittima, nonché
- adottare apposite misure di sicurezza volte a bilanciare tale finalità con i diritti e le libertà fondamentali dei lavoratori,
- redigendo, se del caso (cfr. art. 35 GDPR), anche una valutazione di impatto del trattamento (DPIA).

Laddove la DPIA indichi che i rischi identificati non possono essere sufficientemente affrontati dal responsabile del trattamento (vale a dire che i rischi residui rimangono elevati), il responsabile del trattamento deve consultare l'autorità di controllo prima

[70] Cfr. B. SAETTA, *Privacy e controllo dei lavoratori* in Protezione dati personali.it, pubblicato l'1 Ottobre 2018, 1.

dell'inizio del trattamento (articolo 36, paragrafo 1)[71] come chiarito nelle linee guida del WP29 su DPIA[72].

Nell'ambito di tale valutazione di impatto sulla protezione dei dati personali, il datore di lavoro, indipendentemente dalla tecnologia adottata, dovrà effettuare un cd «test di proporzionalità» («proportionality assessment»), in modo da dimostrare che il trattamento sarà effettuato in misura proporzionata all'attività svolta ed ai diritti e alle libertà fondamenti dell'interessato[73].

In tale ottica, il WP29 ha individuato 9 scenari tipici di trattamento di dati personali dei lavoratori, per lo più basati su un interesse legittimo del titolare del trattamento, che possono presentare dei rischi per i diritti e le libertà fondamentali di questi ultimi[74].

Per ciascuno di tali scenari, il WP29 ha inoltre ricordato che il datore di lavoro deve procedere, nel rispetto dei principi di "*privacy by design"* e "*privacy by default*" previsti dal GDPR, alla previa individuazione della base giuridica del trattamento, alla verifica della necessità delle operazioni di trattamento ed all'esame della correttezza e proporzionalità dello stesso rispetto alle finalità perseguite.

- **Trattamento dei dati dei candidati presenti sui *social network***

Secondo il WP29, il datore di lavoro può trattare i dati dei candidati presenti sui loro profili *social* (opinioni personali, abitudini, interessi, ecc.) solo nelle ipotesi in cui tali profili siano utilizzati dagli interessati per finalità lavorative – e non personali – e laddove gli stessi siano necessari e rilevanti per l'esecuzione della prestazione lavorativa cui la domanda del candidato è rivolta. In tale circostanza, il WP29 ricorda ai datori di

[71] ARTICLE 29 DATA PROTECTION WORKING PARTY, *WP249, Opinion 2/2017 on data processing at work, Adopted on* 8 June 2017, cit., 9.
[72] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is likely to result in "high risk" for the purposes of Regulation 2016/679, WP 248 rev.01,* Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, 18.
[73] Sul punto si veda anche "In sostanza, gli aspetti che emergono con chiarezza dal provvedimento del WP29 sono la concezione della valutazione di rischio come processo e flusso costante; la definizione dell'analisi del rischio come una fase comunque necessaria per ogni trattamento e prima che il trattamento inizi; l'attribuzione esclusiva alla responsabilità del titolare di ogni decisione sia sulla valutazione della elevatezza o meno dei rischi sia dell'eventuale esistenza di rischi così elevati da rendere necessario il ricorso preventivo all'Autorità di controllo" in F. PIZZETTI, *DPIA (Data protection Impact Assessment): cos'è e come fare la valutazione d'impatto in Agendadigitale.eu*, 27 ottobre 2017.
[74] ARTICLE 29 DATA PROTECTION WORKING PARTY, *WP249, Opinion 2/2017 on data processing at work, Adopted on* 8 June 2017, cit., 10.

lavoro di informare preventivamente il candidato del trattamento dei suoi dati personali (mediante, ad esempio, l'inserimento di una specifica indicazione all'interno dell'annuncio di lavoro).

- **Trattamento dei dati dei lavoratori presenti sui *social network***

  Il trattamento dei dati dei lavoratori presenti sui *social network* ha, secondo il WP29, i medesimi presupposti previsti per il trattamento dei dati dei candidati (necessaria pubblicità del profilo *social* dell'interessato, preventiva informativa del trattamento resa agli interessati, sussistenza della necessità e rilevanza del trattamento rispetto al legittimo interesse perseguito). A tal riguardo, tuttavia, il WP29 impone sul datore di lavoro l'onere di provare anche l'insussistenza di strumenti meno invasivi per il raggiungimento delle finalità del trattamento (es.: per il WP29 il datore di lavoro può avere un legittimo interesse a monitorare il profilo Linkedin dell'ex dipendente in regime di non concorrenza con la propria società al fine di verificare il rispetto di tale obbligo da parte dell'ex dipendente).

- **Monitoraggio della strumentazione informatica dei lavoratori**

  Il WP29 ritiene che, stante l'evoluzione delle tecnologie informatiche a disposizione dei datori di lavoro (*Data Loss Prevention, Next-Generation Firewalls, Unified Threat Managment, eDiscovery technologies, BYOD*), il trattamento dati personali dei lavoratori relativi all'utilizzo della loro strumentazione informatica (es.: e-mail ricevute/inviate; siti web visitati; telefonate effettuate) rappresenti la più grande minaccia per la loro riservatezza.

  Per far fronte a tale minaccia, il WP29 incoraggia i datori di lavoro ad adottare specifiche soluzioni volte a prevenire il ricorso ad accessi "successivi" ai dati dei lavoratori (presenti, ad esempio, nella loro cronologia web e/o nella casella di posta elettronica) e suggerisce, a titolo esemplificativo, misure quali: la predisposizione di un elenco di siti in cui la navigazione è vietata; la previsione di calendari di posta personali; la predisposizione di un'apposita policy per l'uso della strumentazione informatica.

  Sul punto, un particolare esempio di approccio preventivo alla protezione dei dati è stato configurato dal WP29 con riferimento alla procedura di *Data Loss Prevention*, utilizzata dai datori di lavoro al fine di individuare e prevenire la trasmissione non autorizzata di informazioni riservate aziendali. Come chiarito dal WP29, nelle ipotesi in cui un datore di lavoro intenda avvalersi di una simile procedura, egli dovrebbe (i)

informare i lavoratori dell'implementazione della stessa, (ii) determinare, in modo chiaro, le regole sulla base delle quali il sistema informatico qualifica una *e-mail* in uscita come in violazione della riservatezza aziendale e (iii) in caso di effettiva violazione, informarne l'interessato al fine di consentire a quest'ultimo di cancellare – e non inviare – tale comunicazione.

Con particolare riferimento all'utilizzo della strumentazione informatica da remoto (es. BYOD), invece, il WP29 ha previsto che, sebbene l'utilizzo di simili tecnologie comporti grandi vantaggi per i lavoratori, esso presenta anche il rischio di accessi non autorizzati ai dati personali da parte di soggetti terzi. Secondo il WP29, pur avendo la necessità di far fronte a tali rischi, il datore di lavoro non può adottare misure di sicurezza quali il monitoraggio dei movimenti del mouse, l'utilizzo di webcam o di tecnologie di "*screen capture*" – in quanto non proporzionate ed eccessive rispetto alle finalità perseguite – ma deve piuttosto implementare misure di sicurezza che rispettino la riservatezza degli interessati (così, ad esempio, se il datore di lavoro intende accedere agli smartphone dei lavoratori per verificare la perdita di dati personali, dovrebbe evitare l'accesso ad aree "private", quali l'archivio fotografico).

- **Mobile Device Managment**

  Le tecnologie di *Mobile Device Managment* consentono al datore di lavoro di gestire (*rectius*, geolocalizzare, installare *software*/applicazioni, cancellare dati personali) da remoto i dispositivi mobili affidati ai lavoratori. In relazione a tali tecnologie, il WP29 ha previsto che ciascun datore di lavoro debba effettuare una DPIA prima dell'inizio del trattamento, al fine di verificare la necessità del trattamento rispetto alle finalità perseguite e garantire il rispetto dei principi di proporzionalità e sussidiarietà. Come precisato dal WP29, inoltre, il datore di lavoro dovrebbe, da un lato, essere in grado di dimostrare che l'utilizzo di tali tecnologie informatiche non rientra in un più ampio programma di trattamento volto all'esclusivo controllo dell'attività dei lavoratori e, dall'altro, adottare sistemi di registrazione delle informazioni volti a raccogliere i dati personali relativi ai dispositivi mobili dei lavoratori solo in casi eccezionali (es. smarrimento).

  In definitiva, solo una full disclosure sul trattamento dei dati personali, che dovrebbero essere ridotti al minimo (oltre che essere conservati per un periodo limitato e cancellati quando non più necessari) potrà garantire un trattamento lecito.

Manifestamente l'intento sia del Garante che del WP29 è quello di guidare e accompagnare il titolare del trattamento (nella fattispecie, il datore di lavoro) nell'adeguamento alle disposizioni europee in materia di tutela della privacy con riguardo al trattamento dei dati personali, indicando misure e strategie concrete idonee a rendere i prodotti e i sistemi conformi ai principi di minimizzazione dei dati, di privacy by design e privacy by default.

4. Modalità operative, *best practice* e indicazioni giurisprudenziali.

«*Due semplici operazioni permettono al lavoratore di essere controllato sui Social network: la creazione di un profilo identificativo (pubblicazione di contenuti e personalizzazione) e la partecipazione (interazione) attiva ad una societas virtuale*»[75].

La complessità deriva dal fatto che l'esercizio del potere di controllo datoriale deve confrontarsi con le impostazioni di privacy del profilo prescelte dal lavoratore, che, infatti, può stabilire e decidere quale grado di pubblicità attribuire al proprio profilo.

Quando il profilo del dipendente sia accessibile solo a "conoscenti" e non sia quindi indiscriminatamente visitabile da chiunque, qualsiasi contenuto pubblicato sulla pagina personale è da considerare riservato: essendo una scelta consapevole di esercitare uno *ius escludendi alios* rispetto alle proprie informazioni personali, la comunicazione è riservata solo ai soggetti specificamente autorizzati dal titolare del dato. Al contrario, quando il profilo sia "pubblico" o comunque "visibile agli amici degli amici", *postare* sul Social equivale a renderlo noto alla collettività in un «luogo aperto al pubblico»; di conseguenza il dato è attingibile da chiunque e quindi anche dal datore di lavoro.

Il nuovo art. 4 St. lav., come è già stato messo in evidenza, ha trasformato il controllo a distanza finalizzato ad accertare comportamenti illeciti ed inadempienti in controllo indiretto sulla prestazione lavorativa. Con la finalità ultima di assoggettare anche questa ipotesi normativa alle garanzie di carattere sostanziale e procedurale già previste dal previgente testo della norma e, al contempo, sottrarla all'imprevedibile ed oscillante giurisprudenza che dominava la materia[76].

[75] Cfr. A. INGRAO, Il controllo a distanza effettuato mediante Social network, in LLI, Vol. 2, No. 1, 2016, ISSN: 2421-2695, cit., 105.
[76] Cfr. A. INGRAO, *Il controllo a distanza effettuato mediante Social network,* in LLI, Vol. 2, No. 1, 2016, ISSN: 2421-2695, cit., 118.

Allorquando il comportamento inadempiente del lavoratore (abuso del *wifi* aziendale per accedere ai Social o distrazione del tempo di lavoro per finalità estranee all'adempimento delle mansioni) sia dovuto all'utilizzo del Social network, il datore di lavoro potrà giovarsi delle funzioni di controllo proprie del web 2.0 (geolocalizzazione, memorizzazione dell'orario dei *post*, visibilità pubblica dei contenuti di quest'ultimi) solo quando queste ultime siano state autorizzate da un accordo sindacale (o da un provvedimento della DTL competente per territorio) che accerti l'esigenza aziendale di tutelare il patrimonio aziendale e a condizione che il lavoratore sia informato di questa modalità di controllo a distanza[77].

Anche indipendentemente dal rapporto di collegamento social (ad es."amicizia" su Facebook), quando il "*profilo privacy*" scelto e adottato dal lavoratore consente visualizzazione dei suoi "post", commenti e foto da parte di tutti (cioè è aperto ad una cerchia di utenti indeterminabile), per il Garante della Privacy è legittimo l'uso a fini disciplinari, da parte del datore di lavoro, di ogni manifestazione "tracciata" da parte del dipendente. Viceversa, ove il profilo di privacy del lavoratore limitasse l'accesso ai dati e il datore di lavoro non avesse dunque legittimamente accesso ai contenuti in questione, si porrebbe l'esigenza di verificare quando, e a che titolo, il datore di lavoro può utilizzare dati ad accesso limitato. «L'interrogativo acquista particolare rilevanza in caso di impugnativa giudiziale, da parte del lavoratore, di una sanzione disciplinare irrogata nei suoi confronti sulla opinabile base di tali presupposti di fatto».[78]

Nella pratica, il datore di lavoro valuta se i comportamenti tenuti dal lavoratore sui social network abbiano o meno leso sotto il profilo disciplinare il rapporto fiduciario: in caso affermativo, può essere comminata finanche la sanzione espulsiva. Nel compiere tale valutazione, occorre tener conto anche di tutte le circostanze che qualificano la fattispecie: inquadramento del lavoratore, ruolo, competenze professionali implicate, limitazioni della privacy, contenuti e stile della comunicazione.

I provvedimenti disciplinari sono sempre applicabili con un principio di gradualità, in relazione alla gravità o recidività della mancanza o al grado della colpa, sicché un licenziamento disciplinare comminato in conseguenza di una violazione che non sia

[77] Cfr. A. INGRAO, *Il controllo a distanza effettuato mediante Social network*, in LLI, Vol. 2, No. 1, 2016, ISSN: 2421-2695, cit., 118-119.
[78] Cfr. D. IODICE, R. COLOMBANI, *Social network e responsabilità disciplinari: le possibili tutele individuali*, in bollettino ADAPT del 17 luglio 2018, n. 27, cit., 3-4.

tale da giustificare il provvedimento espulsivo, può essere considerato illegittimo e censurato dal giudice. Ecco che per la valutazione dei confini del legittimo esercizio del potere disciplinare bisogna sempre esercitare il bilanciamento tra *diritto di critica* e *dovere di fedeltà* e di riservatezza. E l'equo contemperamento di interessi sarà oggetto di apprezzamento giudiziale a seguito dell'impugnativa del provvedimento disciplinare, determinando un ulteriore elemento di incertezza: «altro è esercitare un controllo c.d. "difensivo", a tutela del patrimonio aziendale (allo scopo di accertare violazioni di specifici doveri contrattuali), altro è effettuare controlli sui social network relativamente a fatti e a dati personali non rilevanti»[79].

La Cassazione ha più volte parificato le dichiarazioni rese dal lavoratore a mezzo degli strumenti di comunicazione pubblica quali giornali, radio, televisione a quelle formulate sui social network, confermando l'orientamento per cui il diritto di critica soggiace a stringenti limiti in costanza del rapporto di lavoro, in particolare attinenti a:

a) continenza verbale (correttezza espressiva);

b) continenza sostanziale (verità dei fatti);

c) rilevanza sociale delle dichiarazioni, rispetto allo status del dichiarante e alla sua platea di riferimento.

Il punto a) concerne la "forma" delle dichiarazioni rese sui social, l'uso di espressioni o di toni sproporzionatamente sdegnati e polemici e inadeguati rispetto ai contenuti e come tale può essere specifico presupposto di sanzione disciplinare. E ciò indipendentemente dal destinatario di tali dichiarazioni, che possono essere ritenute in sé incompatibili con lo status di lavoratore in aziende particolarmente esposte ai giudizi del mercato e dell'opinione pubblica in termini di *Brand reputation*, o ultimamente anche di indicatori ESG.[80]

---

[79] Cfr. D. IODICE, R. COLOMBANI, *Social network e responsabilità disciplinari: le possibili tutele individuali*, in bollettino ADAPT del 17 luglio 2018, n. 27, cit., 4-5.

[80] Ad es. «*Molti investitori desiderano che gli aspetti relativi a tematiche ambientali, sociali e di governance (ESG) siano integrati nel processo di investimento poiché ritengono che questi possano generare risultati finanziari superiori tramite la mitigazione dei rischi reputazionali, operativi e finanziari. Secondo PwC nel mondo, le masse complessive dei fondi comuni d'investimento cosiddetti ESG saliranno tra il 2017 e il 2025 di un CAGR pari all'8,5%, raggiungendo 2,08 trilioni di dollari. La ricerca evidenzia che gli investimenti ESG rappresentano il terzo fattore chiave per gli investitori intervistati, superando il tema commissionale; lo dimostra il fatto che le variabili ESG sono passate al vaglio degli analisti e agenzie di rating e quest'area rappresenta attualmente una priorità fondamentale per gli investitori sofisticati in tutto il mondo*.» in M. TESSA, *ESG: priorità per gli investitori. Conta più delle commissioni* in *wallstreetitalia.com*, pubblicato il 13/11/19, 2.

Sul punto b), la descrizione di contenuti non veri o di circostanze non obiettive, così come le dichiarazioni diffamatorie possono di per sé giustificare una sanzione disciplinare. Persino la rappresentazione di contenuti in sé veri e obiettivamente riportati può esporre a conseguenze di natura disciplinare, se le relative informazioni sono oggetto di riserva di confidenzialità o segretezza, nel caso ad es. di prescrizioni contenute nei regolamenti aziendali e/o disciplinari interni (che sono fonti di produzione normativa unilaterale)[81]. In realtà sarebbe prudente non riferire mai sui social di fatti o dichiarazioni aziendali.

Riguardo, infine, alla rilevanza sociale delle dichiarazioni (sub c), essa può valere piuttosto come circostanza aggravante o attenuante della responsabilità disciplinare. Quando esistono i presupposti sub a) e/o b), infatti, qualifica la fattispecie anche lo status del lavoratore: «l'intensità del vincolo fiduciario misura anche, infatti, il grado di responsabilità disciplinare, in modo direttamente proporzionale».[82]

Addirittura, si è visto come con la sentenza 10955 del 27 maggio 2015 la Corte di Cassazione abbia legittimato i datori di lavoro alla creazione di falsi profili Facebook per verificare l'accesso ai social network dei dipendenti durante l'orario di lavoro.

La Corte Suprema ha giustificato il controllo ritenendolo difensivo e volto ad ostacolare commissione di atti illeciti, non facendolo rientrare in questo modo nell'applicazione dell'articolo 4 dello Statuto dei lavoratori.

Secondo la Corte, infatti il controllo, effettuato in buona fede, è stato realizzato con modalità non eccessivamente invasive e rispettando le libertà e la dignità del dipendente.[83]

---

[81] Cfr. «*nel nuovo contesto diventano essenziali i regolamenti interni (le cd. policy aziendali) tramite i quali il datore di lavoro con riferimento ad ogni strumento utilizzato (applicazioni software, accessi ad internet, posta elettronica ecc.) dovrà specificare le modalità del controllo e le cautele volte a minimizzarne l'impatto sulla sfera privata e l'attività del lavoratore (per es. esclusione di controlli continuativi; filtri per bloccare l'accesso a certi siti; trattamento di dati in forma anonima ed aggregata ecc.). Tali regolamenti interni – la norma è esplicita sul punto – dovranno essere comunicati in modo tale che ogni singolo lavoratore possa acquisirne effettiva conoscenza*» in M.T. CARINCI, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23D. Lgs. 151/2015): spunti per un dibattito* in LLI, Vol. 1, No. 1, 2015.

[82] Cfr. D. IODICE, R. COLOMBANI, *Social network e responsabilità disciplinari: le possibili tutele individuali*, in bollettino ADAPT del 17 luglio 2018, n. 27, cit., 5.

[83] Cfr. « *1.9. - Infine, è stato precisato che le norme poste dalla L. 20 maggio 1970, n. 300, artt. 2 e 3, a tutela della libertà e dignità del lavoratore, delimitano la sfera di intervento di persone preposte dal datore di lavoro a difesa dei suoi interessi con specifiche attribuzioni nell'ambito dell'azienda (rispettivamente con poteri di polizia giudiziaria e di controllo della prestazione lavorativa), ma non escludono il potere dell'imprenditore, ai sensi degli artt. 2086 e 2104 c.c., di controllare direttamente o mediante la propria organizzazione gerarchica o anche attraverso personale esterno - costituito in ipotesi da dipendenti di una agenzia investigativa - l'adempimento delle prestazioni lavorative e quindi*

Attenzione però: la falsa creazione del profilo Facebook, che in questo caso è stato accolto positivamente dalla Corte di Cassazione, in altri casi simili potrebbe anche portare a contestazioni per la violazione dell'articolo 494 del codice penale per quel che riguarda il reato di sostituzione di persona.[84]

Alla fine emerge una considerazione, tutto sommato di buon senso: nell'ambito lavorativo, il dipendente deve prestare la massima attenzione a tutte le azioni che pone in essere, anche virtuali, mantenendo una condotta che dovrà essere valutata come decorosa, senza azzardi e rispettosa delle obbligazioni assunte in sede di sottoscrizione del contratto di lavoro, a maggior ragione se si considera che tramite l'uso dei social network i comportamenti attuati possono avere risonanza pubblica. E per giunta fortemente negativa laddove l'utente stesso non dimostri la necessaria consapevolezza sul mezzo impiegato e sulle insidie che vi si celano.

In definitiva, l'autonomia e la tutela della *privacy* del dipendente sono riposte nelle sue stesse mani, in quanto, ove l'utilizzo del mezzo social si riveli corretto, scrupoloso e accorto, il dipendente stesso avrà salvaguardato il suo diritto alla riservatezza, ma anche e soprattutto non avrà compromesso il proprio rapporto di lavoro.

5. Considerazioni finali.

Onde pervenire all'implementazione del controllo a distanza mediante social network l'azienda deve porre molta attenzione in un articolato piano di *data protection compliance*.

Deve adottare un sistema che è concepito, sin dalla fase di progettazione, per fornire uno strumento legittimo e utile a soddisfare le specifiche esigenze organizzative, produttive e di sicurezza sul lavoro nel rispetto dei principi di pertinenza e di non eccedenza espressamente previsti dai «vecchi» provvedimenti sul tema del Garante per la Protezione dei dati personali (antecedenti al GDPR), dall'art. 4 dello Statuto dei Lavoratori (Legge 300/1970) così come modificato dal D. Lgs. n. 151/2015 (attuativo di una delle deleghe del cd. Jobs Act) e più in generale dallo stesso GDPR.

---

di accertare mancanze specifiche dei dipendenti già commesse o in corso di esecuzione, e ciò indipendentemente dalle modalità del controllo, che può avvenire anche occultamente, senza che vi ostino né il principio di correttezza e buona fede nell'esecuzione dei rapporti né il divieto di cui alla stessa L. n. 300 del 1970, art 4, riferito esclusivamente all'uso di apparecchiature per il controllo a distanza (Cass. 10 luglio 2009, n. 16196). », Sentenza cit., 3.

[84] Cfr. P. DEL PIDIO, *Controllo a distanza dei lavoratori: i social network possono essere lo strumento* - InvestireOggi.it, pubblicato il 07 Ottobre 2016.

Uno dei punti più qualificanti in ottica *privacy by design & by default* riguarda la possibilità di modulare l'ampiezza del controllo, aspetto che può fungere plasticamente da cerniera tra possibilità offerte dalla tecnica, secondo le best practice, e necessità di tutele imposte dal diritto[85][86].

In relazione alle finalità perseguite, la società deve muoversi sempre in base al principio di proporzionalità, necessità e minimizzazione dei dati, ai sensi dell'art. 5, par.1, lett.c) GDPR, a salvaguardia delle esigenze di privacy dei lavoratori[87], in un mondo ormai pervaso dal «*capitalismo di sorveglianza», in cui «un altro aspetto radicale riguarda la distribuzione dei diritti alla privacy e con essa la conoscenza e la scelta di accedere a "Big Other". (...) In realtà, privacy e segretezza non sono opposti ma piuttosto momenti di una sequenza. (...) Esercitare il proprio diritto alla privacy produce scelta e si può scegliere di mantenere qualcosa di segreto o di condividerlo. I diritti alla privacy conferiscono quindi diritti di decisione; la privacy consente di decidere dove si vuole essere nello spettro tra segretezza e trasparenza in ogni situazione*» [88].

Ecco perché i regolatori hanno avvertito fortemente la necessità di porre limiti alla tecnica, quella che la stessa Zuboff ha «*chiamato la dimensione materiale di potere[89] in cui sistemi impersonali di disciplina e controllo*» (come già aveva intuito Deleuze) «*producono una certa conoscenza del comportamento umano indipendentemente dal consenso*».

[85] Cfr. «*Ecco il ruolo più significativo in un contesto geopolitico in cui domina il potere dell' algoritmo: ridisegnare, proprio a partire dalla protezione dei dati, i confini del tecnicamente possibile alla luce di ciò che è giuridicamente ed eticamente accettabile*» in S. GUIDA, *I confini del digitale. Nuovi scenari delineati dal Garante per la privacy dopo la Giornata Europea della protezione dei dati personali*, in *ICT Security Magazine - La Prima Rivista Dedicata alla Sicurezza Informatica*, 5 Aprile 2019, 3.
[86] Cfr. M. CHESSELL, *Ethics for big data and analytics*, in *https://www.ibmbigdatahub.com/sites/default/files/whitepapers/reports_/file /TCG /Study Report-Ethics for BD&A.pdf.*, 1.
[87] Cfr. «*La rete dei legami tra diritto, tecnica e potere presenta, d'altro canto, aspetti di notevole ambiguità, visto che la tecnica stessa può svolgere e, di fatto, svolge anche un importante ruolo di contenimento degli eccessi del potere. Come ha scritto Predieri, infatti, "le norme tecniche sono regole indispensabili ad un'economia poliarchica organizzata o sociale di mercato"; esse, adempiendo a una funzione di "eterocorrezione del mercato" e ponendosi a presidio di beni come la salute, la sicurezza dei lavoratori e dei consumatori o l'ambiente, "hanno un ruolo di potere (o di contropotere) nell'equilibrio dei poteri*» in A. MORELLI, *Diritto, scienza e tecnica: la prospettiva del costituzionalista. Recensione ad A. Iannuzzi, Il diritto capovolto. Regolazione a contenuto tecnico- scientifico e Costituzione*, in *Rivista di Diritti Comparati*, N. 1/2019, 205.
[88] Cfr.. S. ZUBOFF, *Big other: surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology* (2015) 30, 82–83.
[89] *Ibidem*, pag. 81.

Ed ecco perché il Garante europeo della protezione dei dati (GEPD) ha avvertito la necessità di un forte richiamo all'etica[90]: «*Le iniziative a sostegno del diritto alla privacy possono fungere da faro per l'integrazione dei principi etici nella progettazione di Internet e della società basata sulla tecnologia per l'intera gamma dei diritti umani. Il GEPD considera la spinta a un'efficace attuazione dei principi della privacy by design e by default come un'opportunità senza precedenti per rafforzare il rispetto dell'etica nella tecnologia. Tutti gli stakeholder hanno una responsabilità importante; in particolare, le società che basano la propria attività sull'utilizzo dei dati personali e le autorità pubbliche sono chiamate a modellare le loro operazioni al servizio del bene comune*».

[90] EUROPEAN DATA PROTECTION SUPERVISOR, *Preliminary opinion on privacy by design. Opinion 5/2018*, 31 maggio 2018 in *https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_ on_privacy_ by_design _en_ 0.pdf* , cit., 20-21.

LA VIDEOSORVEGLIANZA NEL LAVORO.

di Giuliano Palma

SOMMARIO. 1. Inquadramento normativo. 2. Incombenti. 3. I più recenti orientamenti europei. 4. Conclusioni.

This paper focuses on two distinct opposing interests: the protection of private property, and the protection of personal data.
The assembly of video surveillance system should act as a deterrent and, at the same time, allow - for example, in the event of theft - to trace, through the investigative activity of the Police Force, the perpetrators of the crimes.
It is note that the legislative framework is not homogeneous and constituted by provisions of both soft and hard law issued at different times.

1. **Inquadramento normativo**

«*Innanzitutto, con il termine "videosorveglianza" si definisce l'acquisizione, in modo continuativo, di immagini, eventualmente associate a suoni, relative a persone identificabili. Spesso, il rilevamento comporta anche una contestuale registrazione ed una successiva conservazione dei dati*»[91]. Le norme applicabili sono:

- il Provvedimento Generale dell'8 aprile 2010 del Garante Privacy[92];
- il Regolamento Europeo 2016/679/UE, sintetizzato in GDPR[93];
- il Parere Gruppo di Lavoro Art. 29 (ora EDPB, European Data Protection Board o Comitato europeo per la protezione dei dati) n.2/2017 dell'8 Giugno 2017 sul trattamento dei dati dei lavoratori nei luoghi di lavoro – WP 249[94];

[91] Cfr. *https://www.altalex.com/documents/news/2016/12/13/videosorveglianza-geolocalizzazione-e-tutela-della-privacy*
[92] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI,, Provvedimento in materia di videosorveglianza - 8 aprile 2010 [1712680] *(Gazzetta Ufficiale n. 99 del 29 aprile 2010).*
[93] Regolamento (Ue) 2016/679 Del Parlamento Europeo E Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in Gazzetta ufficiale dell'Unione europea del 4 maggio 2016.
[94] ARTICLE 29 DATA PROTECTION WORKING PARTY (ora EDPB), WP 249, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017.

- le Linee guida sul trattamento di dati personali attraverso sistemi di videosorveglianza (Guidelines 3/2019 on the processing of personal data through video devices) adottate dall'European Data Protection Board in data 13 luglio 2019[95].

Con l'avvento del GDPR si è provveduto ad "armonizzare" il Codice Privacy (d.lgs. 196/2003 a mezzo del d.lgs. 101/2018[96]. Ci si augura comunque, un futuro intervento legislativo o dello stesso Garante per chiarire la materia in maniera organica e definitiva.

2. **Incombenti**

«*Da un'analisi complessiva della normativa vigente (compresi i Provvedimenti generali del Garante), risulta che, prima di attivare qualsivoglia sistema di videosorveglianza, è necessario porre in essere una serie di determinati adempimenti*»[97]. «*L'attività di videosorveglianza, in generale, può diventare estremamente invasiva e per questo motivo l'Autorità Garante per la Protezione dei Dati Personali ha emanato nel tempo diversi provvedimenti generali atti a regolarizzarne l'utilizzo*»[98]. Un primo provvedimento risale al novembre 2000[99]: "*In presenza di una crescente utilizzazione di impianti di videosorveglianza da parte di molti soggetti pubblici e privati, il Garante, nell'attesa di una specifica legislazione, reputa necessario sintetizzare gli adempimenti, le garanzie e le tutele già necessari in base alle norme vigenti, per facilitarne la conoscenza da parte degli operatori interessati*"[100]. In tale documento era previsto un "decalogo" comportamentale del seguente tenore:

- Tutti gli operatori interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti.

---

[95] EDPB PLENARY MEETING, *09-10 July 2019, Guidelines 3/2019 on processing of personal data through video devices. Version for public consultation*. 10 luglio 2019.
[96] Decreto Legislativo 10 Agosto 2018, N. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Gazzetta Ufficiale Serie Generale n.205 del 4 settembre 2018. Entrata in vigore del provvedimento: 19/09/2018.
[97] Cfr. *https://www.altalex.com/documents/news/2016/12/13/videosorveglianza-geolocalizzazione-e-tutela-della-privacy*
[98] Cfr. *https://www.agendadigitale.eu/sicurezza/videosorveglianza-post-gdpr-norme-obblighi-e-sanzioni/*
[99] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000.
[100] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000, pag.1.

- Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi.
- Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art.7 legge 675/1996[101]), questi devono indicare anche la raccolta di informazioni mediante apparecchiature di videosorveglianza.
- Si devono fornire alle persone che possono essere riprese indicazioni chiare, che avvertano della presenza di impianti di videosorveglianza ai sensi dell'art. 10 della legge n. 675/1996[7].
- Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori. Tale principio è stato di recente modificato dalla circolare INL n. 5 del 19 febbraio 2018[102].
- Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
- Occorre determinare con precisione il periodo di eventuale conservazione delle immagini.
- Occorre designare per iscritto i soggetti – responsabili e incaricati del trattamento dei dati (artt. 8 e 19 della legge 675/1996)[7] – che possono utilizzare gli impianti e prendere visione delle registrazioni.
- I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori, salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi.

  Successivamente poi, il Garante ha emesso un provvedimento generale l'8 aprile 2010[103], a sostituzione di altro e precedente provvedimento adottato del 2004[104], con

[101] Il quadro legislativo era rappresentato dalla Legge n. 675 del 31 dicembre 1996 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (Pubblicato sulla Gazzetta Ufficiale n. 5 dell´8 gennaio 1997 - Suppl. Ordinario n. 3), legge abrogata ai sensi dell'articolo 183, comma 1, lettera a), del Codice in materia di protezione dei dati personali. Oggi pertanto tale obbligo di notificazione non è più previsto.

[102] Ispettorato Nazionale del Lavoro, Circolare n. 5 del 19 febbraio 2018, avente ad oggetto "*indicazioni operative sull'installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo ai sensi dell'art. 4 della legge n. 300/1970*".

[103] Vedi *supra*..

[104] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Videosorveglianza - Provvedimento generale - 29 aprile 2004 [1003482]. Notevole la "*Premessa: Il Garante ritiene opportuno aggiornare e integrare*

il quale sono stati fissati requisiti più stringenti volti a contemperare le libertà dei cittadini, con le esigenze di sicurezza. Innanzitutto, la videosorveglianza è consentita a condizione che siano rispettati alcuni principi:

- la videosorveglianza deve essere lecita; ad esempio, deve essere predisposta nel rispetto dell'art. 11 del d.lgs. 196/03[105].
- La videosorveglianza deve essere necessaria e proporzionata; non potrò utilizzare sistemi di videosorveglianza se il mio obbiettivo può essere raggiunto con modalità diverse (cfr. art. 11 d.lgs. 196/03[12 106]).
- La videosorveglianza deve avere finalità chiare, prestabilite e legittime.

a) L'obbligo di informativa

Sono inoltre stabiliti specifici adempimenti applicabili a soggetti pubblici e privati. Primo fra tutti l'obbligo di informativa: gli interessati devono essere sempre informati di stare per accedere in una zona videosorvegliata. L'informativa può essere rilasciata mediante il modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita. In presenza di più telecamere, potranno essere installati più cartelli. Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche in orario notturno;

il provvedimento del 29 novembre 2000 (c.d. "decalogo" pubblicato sul Bollettino del Garante n. 14/15, p. 28), anche per conformare i trattamenti di dati personali mediante videosorveglianza al Codice entrato in vigore il 1° gennaio 2004 e ad altre disposizioni vigenti (art. 154, comma 1, lett. c), d.lg. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali) che hanno rafforzato le garanzie per i cittadini. Per altro verso va evidenziato che nel triennio di applicazione del predetto provvedimento sono stati sottoposti all'esame dell'Autorità numerosi casi, attraverso reclami, segnalazioni e richieste di parere, i quali evidenziano un utilizzo crescente, spesso non conforme alla legge, di apparecchiature audiovisive che rilevano in modo continuativo immagini, eventualmente associate a suoni, relative a persone identificabili, spesso anche con registrazione e conservazione dei dati".

[105] Recante il "*Codice in materia di protezione dei dati personali*", in vigore prima che venisse integrato con le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, *ut supra*.

[106] Si pensi, ad esempio, al caso in cui si volessero installare telecamere in un parcheggio, per scongiurare il rischio di furti, danneggiamenti o atti di vandalismo verso i veicoli: in tale ipotesi, i dispositivi video dovranno essere posizionati in modo da limitare l'angolo visuale all'area da tutelare (pertinenza), ai beni che ivi si trovano (completezza), evitando la ripresa di luoghi circostanti e di particolari non rilevanti (non eccedenza). Tale ricostruzione esemplificativa è di A. FROSINI, *La disciplina generale della videosorveglianza*, in M. ALOVISIO, D. BURRONI, A. FROSINI, E.O. POLICELLA, *Videosorveglianza e* privacy, Forlì, 2011, p. 18.

- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione[107].

b) L'obbligo di verifica preliminare e tempi di conservazione dei dati

Altro obbligo stabilito nel Provvedimento in esame era la "verifica preliminare". Fino al d.lgs. 101/2018 era ancora previsto[108] che i trattamenti di dati personali nell'ambito di una attività di videosorveglianza dovessero essere effettuati rispettando le misure e gli accorgimenti prescritti dal Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (art. 17 del Codice privacy[12]), quando vi erano rischi specifici per i diritti e le libertà fondamentali. Un ulteriore caso in cui si rendeva necessario richiedere una verifica preliminare riguardava l'allungamento dei tempi di conservazione dei dati delle immagini registrate oltre il previsto termine massimo di sette giorni derivante da speciali esigenze di ulteriore conservazione, a meno che non derivi da una specifica richiesta dell'autorità giudiziaria o di polizia giudiziaria in relazione a un'attività investigativa in corso.

Quanto alle misure di sicurezza da adottare, si precisa che i dati raccolti mediante sistemi di videosorveglianza dovevano essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta (artt. 31 e ss. del Codice privacy)[12]. Le misure di sicurezza minime richieste del Garante dovevano rispettare i seguenti principi:

- in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. I predetti soggetti, designati incaricati o responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare unicamente le operazioni di propria competenza;

---

[107] Cfr. *https://www.agendadigitale.eu/sicurezza/videosorveglianza-post-gdpr-norme-obblighi-e-sanzioni: "Il Garante ritiene auspicabile che l'informativa, resa in forma semplificata, poi rinvii a un testo completo contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice Privacy (poi modificato con il decreto di recepimento del Regolamento Europeo n. 679/2016 sulla Protezione dei Dati, il Gdpr), disponibile agevolmente senza oneri per gli interessati, con modalità facilmente accessibili anche con strumenti informatici e telematici. In ogni caso il titolare, anche per il tramite di un incaricato, ove richiesto è tenuto a fornire anche oralmente un'informativa adeguata, contenente gli elementi individuati dall'art. 13 del Codice privacy. La violazione delle disposizioni riguardanti l'informativa (omissione o inidoneità), era punita con la sanzione amministrativa prevista dall'art. 161 del Codice medesimo*".

[108] Come dimostrato, ad esempio, dal Provvedimento del Garante per la protezione dei dati personali n. 102 del 22 febbraio 2018, "*Verifica preliminare. Installazione di un sistema di videosorveglianza - 22 febbraio 2018*".

- laddove i sistemi siano configurati per la registrazione e successiva conservazione, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- per quanto riguarda il periodo di conservazione devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
- nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele;
- qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-*ter* del codice penale;
- la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione wireless.

  Inoltre, il titolare o il responsabile del trattamento devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo (art. 30 del Codice)[12] che ad accedere e operare sui sistemi di videosorveglianza. Infine, nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (v. art. 11, comma 1, lett. e), del Codice)[12], anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario – e predeterminato – a raggiungere la finalità perseguita»[109].È chiaro, a questo punto, come sia necessario far luce sul rapporto tra il provvedimento generale del 2010 fin qui esaminato e il GDPR oggi operante, al fine di giungere ad un "combinato disposto".

c) Il Titolare del trattamento e la conseguente responsabilizzazione

Il soggetto pubblico o privato che tratta dati personali mediante videosorveglianza è titolare del trattamento dei dati, ossia la persona (fisica o) giuridica che determina le

[109] Cfr. *https://www.agendadigitale.eu/sicurezza/videosorveglianza-post-gdpr-norme-obblighi-e-sanzioni/*

finalità e le modalità del trattamento. Su questa figura si innesta il principio di responsabilizzazione (o "accountability"), introdotto dal GDPR[110], che è il concetto fondamentale in quanto il titolare del trattamento è pienamente responsabile delle scelte e delle azioni messe in campo[111] (art. 5.2 GDPR), e deve "darne conto" a tutti i soggetti ai quali appartengono i dati trattati (interessati), nonché in determinati casi al Garante privacy e all'autorità giudiziaria[112]. Con il GDPR si diventa *ipso iure* unico centro di imputazione per qualsiasi trattamento non a norma di legge.

d) Le informazioni rese per il trattamento dei dati

La materia della videosorveglianza è caratterizzata dalla particolarità della doppia informativa: un'informativa minima (il cartello "Area videosorvegliata"), che, *ut supra,* ex art. 13 comma 3 dell'abrogato Codice Privacy; ed un'informativa completa[113] da rendersi conforme a quanto disposto dal GDPR. La *ratio* dell'informativa minima è fare in modo che gli interessati siano sempre informati al momento dell'accesso ad una zona videosorvegliata. Venne creata una sorta di "pre-informativa", ossia un cartello che recasse le informazioni più utili ed immediate per l'interessato (indicazione del titolare e della finalità del trattamento). Se l'interessato avesse voluto approfondire, il titolare del trattamento avrebbe dovuto fornire tempestivamente l'informativa completa, senza oneri. In particolare, l'informativa minima, ai sensi del punto 3.1 del provvedimento del 2010 deve: 1) essere collocata prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; 2) avere un formato ed un posizionamento chiaramente visibile in ogni condizione di illuminazione ambientale, anche in orario notturno;3) può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate[114]. Il modello nel Provvedimento dell'8 aprile 2010 prevedeva due versioni[115].

---

[110] Si veda *inter multos* A. PRAITANO, *Privacy by design e GDPR, soluzioni per proteggere i dati in azienda*, cybersecurity360.it, 2018.
[111] Cfr. A. PRAITANO, *op. cit.*, pag.1.
[112] E. ERRICHIELLO, *Il principio di responsabilizzazione e il suo antecedente nel Modello 231*, in *dataprotectionlaw.it*, 2018.
[113] Cfr. M. BUONTEMPI, *Consenso e informativa col GDPR: le basi giuridiche per la compliance,* in *cybersecurity360.it*, 12 novembre 2018, pag.3.
[114]Cfr. *https://www.cybersecurity360.it/legal/privacy-dati-personali/videosorveglianza-e-privacy-le-regole-tra-gdpr-e-provvedimento-generale-del-2010-del-garante/*
[115] Cfr. *https://protezionedatipersonali.it/videosorveglianza-e-tutela-dei-cittadini*

All'informativa minima segue l'informativa "completa" resa ai sensi dell'art. 13 del GDPR, con:

- l'identità e i dati di contatto del titolare del trattamento.
- I dati di contatto del Responsabile della Protezione dei Dati (DPO)[116]se presente.
- Le finalità del trattamento, ovvero:

1. protezione e incolumità degli individui;
2. protezione della proprietà;
3. rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4. acquisizione di prove.

Naturalmente, è necessaria coerenza nell'utilizzo delle medesime finalità del trattamento per l'informativa minima e per l'informativa completa:

- la base giuridica che legittima il trattamento mediante videosorveglianza è l'interesse legittimo (art. 6, comma 1, lettera f del GDPR), una tra le più particolari condizioni di liceità del GDPR[117]";
- i destinatari del trattamento;
- il trasferimento all'estero di dati verso paesi terzi o organizzazioni internazionali. È, inoltre, necessario inserire la presenza o l'assenza di decisioni di adeguatezza della Commissione Europea;
- il periodo di conservazione dei dati o i criteri utilizzati per determinarne il periodo[118];

---

[116] Si veda *inter multos* F. DI RESTA, *Privacy, il DPO: chi è e come nominarlo*, in *agendadigitale.eu*, 2 settembre 2018.

[117] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento del 22 febbraio 2018 - Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679: "Il provvedimento del 2010 al punto 6.2.2. - richiamato dal più recente provvedimento del Garante del 22 febbraio 2018[117] - afferma che "la rilevazione delle immagini può avvenire senza consenso, qualora, con le modalità stabilite in questo stesso provvedimento, sia effettuata nell´intento di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, o finalità di prevenzione di incendi o di sicurezza del lavoro".

[118] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento del 22 febbraio 2018 - *op. cit.*: "*Al punto 3.4 del provvedimento del 2010 si legge che "nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità anche l´eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario – e predeterminato – a raggiungere la finalità perseguita*". Inoltre "*la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo*

- i diritti dell'interessato sui suoi dati personali. Tali diritti sono esercitati dall'interessato senza alcuna formalità e gratuitamente (salvo richieste reiterate, eccessive o infondate); il titolare del trattamento deve ottemperare alle richieste senza ingiustificato ritardo. Inoltre, si risponde, ove possibile, alle richieste dell'interessato nella stessa forma.

  Vediamo quali sono i diritti dell'interessato sui suoi dati personali in materia di videosorveglianza:

1. ai sensi dell'art. 15 GDPR l'interessato ha il diritto di ottenere (gratuitamente) dal titolare del trattamento la conferma che è in atto – o meno – un trattamento di dati personali che lo riguarda, di ottenere l'accesso a questi dati ed alcune informazioni già previste (e garantite) nell'informativa.
2. Ai sensi dell'art. 16 GDPR l'interessato ha il diritto di ottenere la rettifica di dati personali inesatti ovvero l'integrazione di dati personali incompleti.
3. Ai sensi dell'art. 17 GDPR l'interessato ha il diritto alla cancellazione dei suoi dati: 1) nel caso che (a suo avviso) non siano più necessari rispetto alle finalità di raccolta; 2) nel caso si opponga al trattamento e non vi siano altri motivi legittimi per procedere con lo stesso; 3) nel caso i dati siano trattati illecitamente da parte del titolare del trattamento; 4) nel caso i dati debbano essere cancellati per adempiere ad un obbligo di legge cui è soggetto il titolare del trattamento. In tutti questi casi il titolare del trattamento dovrà procedere alla cancellazione di tali dati senza ingiustificato ritardo. Non si applica il diritto alla cancellazione quando vi è l'esercizio del diritto alla libertà di espressione e di informazione; un obbligo di legge da rispettare; un compito da svolgere nel pubblico interesse ovvero l'esercizio di pubblici poteri cui può essere investito il titolare del trattamento; ed infine non si applica per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria (art. 24 Cost.).
4. Ai sensi dell'art. 18 GDPR l'interessato ha il diritto di ottenere la limitazione del trattamento dei dati personali che lo riguardano quando: 1) contesta l'esattezza dei dati

---

in alcuni casi, per peculiari esigenze tecniche o per la particolare rischiosità dell´attività svolta dal titolare del trattamento, può ritenersi ammesso un tempo più ampio di conservazione dei dati che, si ritiene non debba comunque superare la settimana". *Nel rispetto del principio di minimizzazione, dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5.1 lett. c*)".

personali (nei limiti della durata di conservazione); 2) il trattamento è illecito; 3) l'interessato ha necessità di utilizzare i suoi dati per l'accertamento, l'esercizio o la difesa di un suo diritto in sede giudiziaria benché il titolare non abbia più bisogno di questi dati; infine, quando l'interessato si oppone al trattamento dei suoi dati.

5. Ai sensi dell'art. 21 GDPR l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento avente come base giuridica il legittimo interesse, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Inoltre, il diritto di opposizione deve essere portato all'attenzione dell'interessato – e presentato – in maniera chiara e separata da ogni altra informazione al più tardi al momento della prima comunicazione.

- L'informativa privacy deve contenere il diritto di proporre reclamo presso un'Autorità di Controllo.
- L'informativa privacy deve specificare se la comunicazione di dati personali (ai destinatari) è un obbligo di legge o contrattuale, se l'interessato ha l'obbligo di fornire tali dati e le possibili conseguenze nel caso in cui lo stesso non volesse procedere con la comunicazione.
- Infine, l'informativa privacy deve specificare se è in atto un processo decisionale automatizzato (art. 22 GDPR), con la logica utilizzata, l'importanza e le conseguenze di tale trattamento.

e) Le misure di sicurezza per la protezione dei dati

Le misure di sicurezza[119] da adottare in materia di videosorveglianza devono rispettare l'art. 32 GDPR. I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con adeguate (non più "idonee e preventive") misure di sicurezza, riducendo al minimo i rischi, anche in relazione alla trasmissione delle immagini. Devono essere adottate specifiche misure tecniche ed organizzative che consentano al titolare del trattamento di verificare l'attività svolta da parte di chi accede alle immagini o controlla i sistemi di ripresa. Sia i soggetti che rilevano, sia i soggetti che registrano devono possedere credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza. Per quanto

[119] Cfr. D. PADOVAN, *Misure idonee di sicurezza: garantire integrità e riservatezza dei dati*, in *cybersecurity360.it*, 14 dicembre 2018, pag.1.

riguarda il periodo di conservazione delle immagini (a prescindere dalla durata scelta) devono essere predisposte misure tecniche od organizzative per la cancellazione. Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele. Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all´art. 615-ter del codice penale. La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche[120] che ne garantiscano la riservatezza. Le stesse cautele per connessioni wireless.

L'art. 32 GDPR dispone che per approntare delle adeguate misure di sicurezza bisogna tener conto dello stato dell'arte (avanzamento tecnologico), dei costi di attuazione (delle misure di sicurezza), della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (porre in essere, quindi, un'analisi del rischio sui dati personali trattati). Tra le "soluzioni" che l'art. 32 elenca – in maniera non esaustiva – vi sono: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (ovvero, anche la capacità del sistema di resistere e reagire); c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico (es. backup / disaster recovery); d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Inoltre, nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. Inoltre, il titolare del trattamento fa sì che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non tratti tali dati se non è istruito. Misure imprescindibili che precedono quanto previsto dall'art. 32 GDPR sono le seguenti:

- controllo degli accessi alle postazioni PC, nonché ad altri terminali, mediante username e password per ogni singolo operatore del sistema di videosorveglianza;

[120] Cfr. M.CUSCUSA, *Crittografia per le aziende, protette e compliant al Gdpr: ecco come*, in *cybersecurity360.it*, 1 ottobre 2018.

- username e password devono essere perfettamente memorizzati, non vanno scritti su carta e collocati a vista presso la postazione PC, sono personali e non cedibili a nessuno;
- ogni volta che si abbandona la postazione PC, anche per pochi secondi, va effettuata la disconnessione dal terminale (ad esempio, Logo Windows + L);
- la password va cambiata periodicamente, deve essere complessa e non va ceduta a nessuno;
- su ogni PC e terminale vanno installati Antivirus e Firewall con licenze d'uso originali (preferibilmente, non affidarsi a software gratuiti);
- antivirus e firewall devono essere aggiornati quotidianamente;
- dotarsi di soluzioni di crittografia / pseudonimizzazione per gli archivi elettronici;
- porre in essere backup periodici;
- replicare le stesse misure di sicurezza sui terminali mobili (smartphone, tablet ecc. dato che i sistemi di videosorveglianza possono essere gestiti da diversi dispositivi).

Infine, è possibile – anche in ambito videosorveglianza – che il titolare del trattamento subisca un *data breach* (violazione di dati personali – Artt. 33 e 34 GDPR). In caso di *data breach*, il titolare del trattamento deve, senza ingiustificato ritardo e non oltre 72 ore dal momento in cui ne è venuto a conoscenza, notificare la violazione al Garante privacy, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre le 72 ore è necessario allegare alla notifica il motivo del ritardo. La notifica del *data breach* contiene: I) descrizione dettagliata del data breach; II) categorie e numero approssimativo di interessati; III) categorie e numero approssimativo di registrazioni dei dati personali; IV) dati di contatto del titolare del trattamento per tutte le informazioni richieste dal Garante Privacy; V) descrizione delle probabili conseguenze del data breach; VI) descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio. In ogni caso, a prescindere dalla necessità di notifica o meno di un data breach, il titolare del trattamento deve documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente al Garante Privacy di verificare il rispetto di quanto disposto dal GDPR.

f) Videosorveglianza e GDPR: soggetti autorizzati al trattamento dati e responsabili esterni

Parafrasando il punto 3.3.2 del provvedimento del 2010, il titolare del trattamento deve designare per iscritto tutte le persone fisiche autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, a visionare le immagini. Ai sensi dell'art. 2-quaterdecies del Codice Privacy il titolare o il responsabile del trattamento possono prevedere, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

Le persone autorizzate al trattamento dei dati personali rilevati da un sistema di videosorveglianza e che operano sotto l'autorità del titolare o del responsabile dovranno ricevere istruzioni adeguate e attenersi a quanto impartito dal titolare o dal responsabile, pena anche provvedimenti di natura disciplinare.

Qualora il titolare del trattamento abbia invece necessità di "appaltare" il trattamento di videosorveglianza ad altro soggetto, quest'ultimo rivestirà la "carica" di responsabile del trattamento. Il rapporto tra il titolare e il responsabile del trattamento – ex artt. 28 e 29 GDPR – deve essere obbligatoriamente sancito da un contratto o da un altro atto giuridico che abbia la caratteristica di vincolare i due soggetti. Per "delegare" un trattamento il responsabile deve fornire delle "garanzie sufficienti" di compliance al GDPR. La valutazione sul possesso di queste garanzie è "prerogativa" obbligatoria del titolare del trattamento. Il responsabile del trattamento non può ricorrere ad un "sub-responsabile del trattamento" senza la previa autorizzazione scritta del titolare. Inoltre l'autorizzazione del titolare può essere specifica o generale e, in quest'ultimo caso, il responsabile del trattamento informa il titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-responsabili, dando così all'opportunità di opporsi a tali modifiche. Ma quali sono i contenuti che deve possedere il contratto/atto vincolante con il responsabile del trattamento?

- Il responsabile tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
- il responsabile garantisce che le persone autorizzate si siano impegnate alla riservatezza o abbiano un obbligo di riservatezza;

- il responsabile deve adottare tutte le misure di sicurezza adeguate richieste ai sensi dell'articolo 32 GDPR;
- il responsabile si impegna a rispettare quanto disposto per i sub-responsabili del trattamento;
- il responsabile deve assistere il titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste degli interessati;
- il responsabile assiste il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 GPDR;
- il responsabile – su scelta del titolare – deve provvedere alla cancellazione o alla restituzione di tutti i dati personali al termine della prestazione dei servizi relativi al trattamento; il responsabile deve, inoltre, cancellare le copie esistenti, salvo che la legge non preveda la conservazione dei dati;
- il responsabile deve mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi e deve consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati direttamente dal titolare o da un altro soggetto da questi incaricato;
- inoltre, il responsabile del trattamento informa immediatamente il titolare qualora, a suo parere, un'istruzione violi il GDPR o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

  L'atto che vincola il titolare al responsabile è importante in quanto permette di "responsabilizzare il responsabile". Non si dimentichi, però, che l'accountability[121] è propria del titolare e non è delegabile.

g) Videosorveglianza e GDPR: gli specifici settori.

Recentemente il Garante privacy ha inserito "i trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche videosorveglianza e geoloca-

[121] Si veda *inter multos* M. IASELLI, *Il principio di accountability: uno dei pilastri del GDPR*, altalex.com, 13 febbraio 2018.

lizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti" tra i trattamenti soggetti a valutazione di impatto[122]»[123]. È doveroso il coordinamento con la disciplina dettata dallo Statuto dei lavoratori, il quale – all'art. 4, comma 1[124], da considerarsi «la norma di riferimento per l'adozione di sistemi di videosorveglianza in ambito lavorativo»[125] – vieta in modo assoluto il controllo a distanza dei lavoratori[126]. La disposizione, dunque, vieta i cosiddetti controlli intenzionali; invece, dei cosiddetti controlli preterintenzionali si occupa l'art. 4, comma 2, Statuto dei lavoratori, il quale stabilisce che "gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti". «Questa norma, in altri termini, permette la predisposizione di sistemi di videosorveglianza volti a far fronte a esigenze organizzative, produttive o di sicurezza sul lavoro, purché – rispetto alle stesse – il potenziale controllo sull'attività produttiva del lavoratore si configuri come accessorio, ossia come mera conseguenza accidentale, non specificamente voluta (c.d. controllo preterintenzionale, appunto). In tali casi, il datore di lavoro deve, innanzitutto:

- stipulare un accordo con le rappresentanze sindacali in azienda o, in mancanza di esse, con la commissione interna;
- in assenza di accordo, richiedere un provvedimento autorizzativo alla Direzione provinciale del lavoro[127].

---

[122] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018).

[123] Cfr. *https://www.cybersecurity360.it/legal/privacy-dati-personali/videosorveglianza-e-privacy-le-regole-tra-gdpr-e-provvedimento-generale-del-2010-del-garante/*

[124] Statuto dei lavoratori (Legge 300/1970), Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento, aggiornato, da ultimo, con le modifiche apportate dal d.lgs. 24 settembre 2016, n. 185.

[125] Legge 300/1970, art. 4 comma 1: «È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dei lavoratori».

[126] Così, D. BURRONI, A. FROSINI, *La videosorveglianza nel rapporto di lavoro privato*, in M. ALOVISIO, D. BURRONI, A. FROSINI, E.O. POLICELLA, *Videosorveglianza e* privacy, *op. cit.*, p. 72.

[127] Per un'analisi degli aspetti giuridici attinenti alla procedura, D. BURRONI, A. FROSINI, *op. cit.*, p. 77 ss., il quale si dedica anche alla disciplina dei cosiddetti controlli difensivi.

Dopodiché, dovrà osservarsi la procedura, successiva all'eventuale onere di notificazione. In proposito si è recentemente pronunciata la Corte di Cassazione, affermando che "non è soggetta alla disciplina [del citato art. 4, comma 2, Statuto dei lavoratori] l'installazione di impianti e apparecchiature di controllo poste a tutela del patrimonio aziendale dalle quali non derivi anche la possibilità di controllo a distanza dell'attività lavorativa, né risulti in alcun modo compromessa la dignità e la riservatezza dei lavoratori"[128]. In altri termini, secondo i giudici di legittimità, ove la videosorveglianza c.d. difensiva non dia luogo a controlli intenzionali e nemmeno a controlli preterintenzionali, non si rivela necessario – per l'attivazione dei relativi impianti – il consenso delle organizzazioni sindacali»[129]. In mancanza di accordo, gli impianti e gli strumenti di cui sopra possono essere installati previa autorizzazione[130]della sede territoriale dell'Ispettorato nazionale del lavoro (c.d. I.N.L.). A tal proposito, «La circolare dell'Ispettorato Nazionale del Lavoro n. 5 – 19 febbraio 2018 riporta indicazioni operative al personale ispettivo su norme e prassi sia per l'installazione sia per l'utilizzo a norma di impianti audiovisivi ed altri strumenti di controllo. Il provvedimento aggiorna ciò che è stato introdotto dagli articoli 23 del d.lgs. n. 151/2015 e dall'art. 5, comma 2 del d.lgs. n. 185/2016 in materia di videosorveglianza nei luoghi di lavoro. Affronta, nello specifico, 4 aspetti:

1. Istruttoria delle istanze presentate riguardanti la volontà (e necessità) d'installazione di impianti di videosorveglianza specificando ragioni che legittimino il controllo;
2. Tutela del patrimonio aziendale, uno dei motivi che possono giustificare il controllo a distanza dei lavoratori, da determinare con attenzione ed in casi particolari;
3. Telecamere;
4. Dati biometrici: il riconoscimento biometrico installato sulle macchine ne impedisce l'uso a persone non autorizzate ed è quindi, in certi contesti, indispensabile.

Sicurezza sul lavoro, esigenze organizzative e produttive, tutela del patrimonio aziendale sono le uniche finalità che rendono legittima la richiesta di installazione del sistema di videosorveglianza, come da art. 4 dello Statuto dei lavoratori. L'accesso da

[128] Cfr. Cass., sez. Lavoro, 8 novembre 2016, n. 22662.
[129] https://www.agendadigitale.eu/sicurezza/videosorveglianza-post-gdpr-norme-obblighi-e-sanzioni/
[130] Cfr. INL Circolare n°5 del 19 febbraio 2018, pag. 1: "Con la presente circolare, condivisa con il Ministero del lavoro e delle politiche sociali, si forniscono indicazioni operative in ordine alle problematiche inerenti l'installazione e l'utilizzazione di impianti audiovisivi e di altri strumenti di controllo".

remoto alle immagini (in tempo reale o registrate) acquisite dal sistema di videosorveglianza devono essere espressamente autorizzate sulla base di una precisa motivazione. I due tipi di accesso vengono ben distinti dalla nuova circolare:

- l'accesso da remoto alle immagini in tempo reale viene autorizzato solo in casi eccezionali, se debitamente motivato;
- l'accesso alle immagini registrate (da remoto o in loco) va tracciato tramite log, funzione che permette oltretutto l'obbligatoria conservazione dei cosiddetti 'log di accesso' per un periodo non inferiore a 6 mesi.

L'altra importante novità: nell'ambito del provvedimento autorizzativo, non va più posta, come condizione, la necessità della 'doppia chiave fisica o logica (password) per l'utilizzo e l'accesso al sistema. Le norme per la videosorveglianza si applicano anche ai luoghi aziendali esterni con accesso occasionale. Anche se autorizzati dall'INS, i lavoratori devono essere correttamente informati.

h) Il sistema di antifurto nei luoghi di lavoro

La circolare affronta anche un altro aspetto: i sistemi di antifurto nei luoghi di lavoro, che non sono associati al controllo dei dipendenti e l'autorizzazione viene concessa più rapidamente rispetto ai moderni sistemi di videosorveglianza. L'INL ha già chiarito, in passato, un fatto semplice: se videocamere o fotocamere si attivano esclusivamente con l'impianto di allarme inserito, non sussiste l'intenzione a priori di controllare il personale, dunque questa possibilità non rappresenta un motivo di ostacolo per il rilascio del provvedimento di autorizzazione (peraltro rapido). Se, invece, l'azienda richiede l'installazione di un sistema di antifurto in orari di lavoro, quindi in presenza dei lavoratori, può sperare di ottenere l'autorizzazione solo se il controllo invasivo è giustificato da una finalità legittima come la tutela del patrimonio aziendale ed in casi particolari»[131]. Aggiungasi, che: «La Suprema Corte di Cassazione ha, inoltre, decretato che le garanzie poste in materia di divieto di controlli a distanza dal secondo comma dell'articolo 4 dello Statuto siano applicabili anche ai "controlli difensivi", ossia quelli volti ad accertare comportamenti illeciti dei lavoratori nel caso in cui: "tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal

[131] Cfr. *https://www.piusicurezza.com/2018/06/12/videosorveglianza-nei-luoghi-di-lavoro-circolare-inl-n-5-19-febbraio-2018/*

rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso", stabilendo, quindi, che siano legittimi quei controlli diretti ad accertare comportamenti illeciti del lavoratore e lesivi del patrimonio aziendale (per tutte cfr. Cass. n.27093/2018[132] e Cass. n.20879/2018[133]). In pratica, è possibile installare telecamere laddove venga riscontrata una necessità oggettiva ed una finalità precisa volta alla tutela dei beni aziendali, alla sicurezza del lavoro o a specifiche esigenze lavorative secondo i principi di:

- Liceità: ossia per ottemperare ad un obbligo di legge o per tutelare un interesse legittimo.
- Necessità: ossia laddove sia riscontrabile una motivazione che giustifichi l'utilizzo di videocamere di sorveglianza
- Proporzionalità: ossia che l'installazione delle videocamere venga ritenuta una misura proporzionata agli scopi prefissi
- Finalità: ossia che gli scopi prefissi siano determinati, espliciti e legittimi.

L'installazione di videocamere fasulle è vietata ed, anzi, potrebbero crearsi diverse problematiche in quanto verrebbero a mancare i principi, sopra citati, di necessità e proporzionalità: se si è deciso di installare telecamere non funzionanti significa che l'installazione stessa non è reputata necessaria»[134]. Va rimarcato che non è ammissibile il consenso dei dipendenti/lavoratori all'installazione dell'impianto di videosorveglianza in alternativa alla procedura dinanzi l'Ispettorato del lavoro (Cass. Pen. Sez. 3, n. 38882[135] e 38884[136] del 24 agosto 2018).[137][138]

---

[132] Cfr. *http://www.italgiure.giustizia.it/xway/application/nif/20181025*.
[133] Cfr. *http://www.italgiure.giustizia.it/xway/application/nif/20180823*.
[134] Cfr. *https://www.gbsweb.it/blog/videosorveglianza-aziendale/*
[135] Corte di Cassazione, sez. III Penale, sentenza n. 38882/18; depositata il 24 agosto 2018 in dirittoegiustizia.it, 27 agosto 2018. "*La Corte ha deciso di confermare la condanna inflitta dal giudice di primo grado, ritenendo che la mancanza di un accordo sindacale o, in alternativa, di una esplicita autorizzazione dell'Ispettorato configurino, di per sé, una violazione dell'art. 4 dello Statuto dei Lavoratori in materia di installazione di sistemi di videosorveglianza "potenzialmente in grado di controllare a distanza l'attività dei lavoratori, anche nel caso in cui questi ultimi abbiano autorizzato il datore di lavoro ad installare le telecamere*"
[136] Cassazione Penale, Sez. 3, 24 agosto 2018, n. 38884 - Installazione di impianti audiovisivi volti al controllo a distanza dei lavoratori. Estinzione del reato. "*La Cassazione ha ritenuto che ove la "prescrizione" sia stata correttamente e tempestivamente ottemperata dall'azienda (unitamente al pagamento della sanzione amministrativa), il reato debba essere ritenuto estinto*".
[137]CNEL Notiziario Mercato Lavoro ottobre 2018, in cliclavoro.gov.it/Barometro-Del-Lavoro/Documents/2018.
138In:

i) *Il registro dei trattamenti e la valutazione di impatto*

Infine, anche in ambito videosorveglianza trovano largo spazio il registro dei trattamenti[139] e la valutazione di impatto (DPIA), capisaldi del nuovo regolamentoeuropeo. Il titolare e/o il responsabile possono/devono (la differenza tra "l'obbligo e il consiglio" risiede nell'art 30.5 del GDPR) costituire apposito registro – ovvero inserire un'apposita sezione per il trattamento dati videosorveglianza nel Registro preesistente – per la disciplina di tale particolare aspetto. Nel caso si dovesse / volesse procedere con il Registro, il suo contenuto varierà a seconda che lo rediga il titolare o il responsabile.

Nel caso del titolare l'art. 30.1 GDPR prevede le seguenti informazioni:

1. il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento (art. 26 GDPR), del rappresentante (art. 27 GDPR) del titolare del trattamento e del responsabile della protezione dei dati;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
5. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 GDPR, la documentazione delle garanzie adeguate;
6. ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
7. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Nel caso del responsabile, invece, l'art. 30.2 GDPR prevede le seguenti informazioni:

---

https://www.filodiritto.com/news/2018/videosorveglianza-cassazione-penale-il-consenso-dei-lavoratori-non-sostituisce-laccordo-sindacale-o-lautorizzazione.html; https://www.lavoroediritti.com/sentenze/installazione-impianti-di-videosorveglianza-non-basta-il-consenso-dei-lavoratori; https://www.certifico.com/categorie/263-news/news-consumers/6168-videosorveglianza-sul-posto-di-lavoro-normativa-e-autorizzazioni

[139] Cfr. *inter multos* LUCA MORINI, *GDPR e registro dei trattamenti: ecco come redigerlo correttamente*, cybersecurity360.it.

1. il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati (DPO – artt. 37-38-39 GDPR);
2. le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
3. ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
4. ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

La valutazione di impatto[140] – artt. 35-36 GDPR – invece, si configura come un'autonoma valutazione che il titolare del trattamento pone in essere per analizzare la necessità, la proporzionalità e i rischi di un determinato trattamento dati per i diritti e le libertà delle persone fisiche. L'art. 35.3 c) GDPR obbliga la conduzione di una valutazione di impatto in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (caso tipico, la videosorveglianza su larga scala). Secondo le Linee - guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)[141], si deve far riferimento al numero degli interessati, al volume di dati e/o tipologie di dati, alla durata dell'attività di trattamento e all'ambito geografico dell'attività di trattamento[142]»[143].

l) Le sanzioni previste in ambito videosorveglianza e GDPR

[140] Cfr. *inter multos* A. D'AGOSTINO, G. GIROTTO, *Il Data Protection Impact Assessment "DPIA": cos'è e come svolgerlo*, diritto24.ilsole24ore.com, 30 gennaio 2018.
[141] Linee - guida del Comitato Europeo per la Protezione dei Dati (già "Gruppo dei Garanti Privacy europei", WP29) concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 rev.01, adottate il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017.
[142] Linee - guida WP29, *op. cit.*, pag. 1 e ss.
[143] Cfr. *https://www.cybersecurity360.it/legal/privacy-dati-personali/videosorveglianza-e-privacy-le-regole-tra-gdpr-e-provvedimento-generale-del-2010-del-garante: "In ogni caso la valutazione d'impatto dovrà contenere: 1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; 2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; 3. una valutazione dei rischi per i diritti e le libertà degli interessati; 4. le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per la protezione dei dati personali, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".*

Il GDPR e il nuovo Codice Privacy introducono un apparato sanzionatorio "misto": il GDPR disciplina le sanzioni amministrative, mentre il nuovo Codice Privacy le sanzioni penali. Il GDPR prevede sanzioni fino a 10.000.000 di euro – o fino al 2% del fatturato mondiale annuo dell'esercizio precedente – per le violazioni degli obblighi di cui agli artt. 8, 11, da 25 a 39, 42 e 43, e 41, paragrafo 4 GDPR. Mentre prevede sanzioni fino a 20.000.000 di euro – o fino al 4% del fatturato mondiale annuo dell'esercizio precedente:

- per le violazioni dei principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9 GDPR;
- per la violazione dei diritti degli interessati a norma degli articoli da 12 a 22 GDPR;
- per la violazione delle disposizioni circa i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49 GDPR;
- per la violazione di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX GDPR;
- nonché per l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo (ad esempio, Garante privacy) ai sensi dell'articolo 58, paragrafo 2 GDPR, o il negato accesso in violazione dell'articolo 58, paragrafo 1 GDPR»[144].

«*La violazione della legge sulla privacy si verifica anche quando: le telecamere sul lavoro sono solo installate ma non ancora funzionanti; è stato dato preavviso ai lavoratori ma non è stato ancora acquisito il consenso dei sindacati; il controllo è discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente. La violazione si configura anche nel caso di telecamere finte montate a scopo esclusivamente dissuasivo. Che succede se le telecamere sono installate senza rispetto delle procedure? I filmati registrati dal datore di lavoro senza il rispetto delle condizioni e delle procedure appena descritte non sono prove: quindi sono inutilizzabili contro il lavoratore in un eventuale processo. La conseguenza è che il licenziamento è illegittimo in quanto non supportato da prove e il dipendente ha diritto alla reintegra sul posto. Non solo. Il datore di lavoro che installa delle telecamere*

[144]Cfr. *https://www.cybersecurity360.it/legal/privacy-dati-personali/videosorveglianza-e-privacy-le-regole-tra-gdpr-e-provvedimento-generale-del-2010-del-garante/*

senza il rispetto delle regole appena elencate commette anche reato[145] *di violazione del divieto di controlli a distanza sui lavoratori. Tale comportamento, inoltre, integra la fattispecie della condotta antisindacale*»[146].

3. **I più recenti orientamenti europei**

Il gruppo di lavoro WP29 ha emanato un proprio parere (Opinion 2/2017 dell'8 Giugno 2017 sul trattamento dei dati dei lavoratori nei luoghi di lavoro – WP 249)[147] aggiornato sul modo in cui deve avvenire il trattamento dei dati personali nei luoghi di lavoro anche in relazione al Regolamento UE 679/16 (GDPR). In particolare il gruppo di lavoro ha mirato ad evidenziare il "bilanciamento tra il legittimo interesse dei datori di lavoro e le ragionevoli aspettative di privacy dei dipendenti, sottolineando i rischi posti dalle nuove tecnologie ed intraprendere una valutazione di proporzionalità di un certo numero di scenari in cui potrebbero essere utilizzati". Dalla lettura del parere si evince un importante nuovo costrutto: non sarà più ritenuto sufficiente l'ottenimento del mero consenso da parte dei dipendenti e dei collaboratori al trattamento dei dati personali effettuato da parte dei datori di lavoro ma occorrerà tenere conto di ciò che il datore di lavoro stesso abbia presunto essere il proprio "legittimo interesse" ad effettuarlo (es. sicurezza aziendale, migliore allocazione delle risorse, ecc.). Inoltre viene anche specificata la portata soggettiva dell'applicazione del parere: a tutti coloro intrattengono una relazione di subordinazione indipendentemente dalla base contrattuale posta in essere tra le parti (es. collaboratori). Tra le condizioni di liceità del trattamento assume ora rilevanza fondamentale per il datore di lavoro rispettare ciò che il GDPR evidenzia anche all'art. 6: "Il trattamento è lecito solo se e nella misura in cui è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato

[145] Corte di Cassazione, Sezione Penale, Sentenza n. 4564/18 del 31.01.2018

146 Cfr. *https://www.laleggepertutti.it/280854_telecamere-sul-posto-di-lavoro: "Secondo la Cassazione, può essere denunciato dai propri dipendenti, per violazione della privacy, l'imprenditore che nasconde una telecamera in un ufficio per spiare ciò che fa il lavoratore, anche se lo fa per evitare che questi rubi. È vero infatti che l'uso della videosorveglianza è possibile nel caso di «controlli difensivi», ma solo se l'uso dell'impianto non lede la dignità del lavoratore (tale sarebbe, ad esempio, una telecamera montata nel bagno o puntata solo su un unico dipendente, allo scopo di controllarne ogni minimo spostamento 8 ore al giorno). Dall'altro lato non si può installare la telecamera-spia con l'intento difensivo se non ci sono validi sospetti del reato del dipendente. La telecamera-spia in funzione "preventiva" è illegale. Inoltre il filmato della telecamera-spia deve essere usato solo per rilevare l'eventuale reato e non per contestare altre condotte, come ad esempio una pausa sigaretta troppo lunga*".

[147] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2017 on data processing at work*, 2007, op. cit.

è un minore", oltre al rispetto di tre principi opportunamente richiamati nel parere stesso: basi legali (ex art. 7 Dir 95/46/CE), trasparenza e decisioni automatizzate. Pertanto oltre alla presenza di una base giuridica lecita affinché, il datore di lavoro, indipendentemente dalla tecnologia adottata, dovrà effettuare un collaudo o "*test di proporzionalità*" (c.d. "*proportionality test*") in modo antecedente all'avvio del trattamento.

Qualora dalla valutazione di impatto dovessero emergere rischiosità elevate il titolare dovrà consultare l'Autorità prima di iniziare il relativo trattamento. Nel parere viene inoltre specificato che:

– i datori di lavoro devono sempre tenere conto dei principi fondamentali della protezione dei dati personali, indipendentemente dalla tecnologia utilizzata;

– i contenuti delle comunicazioni elettroniche effettuate presso i locali commerciali godono delle stesse tutele dei diritti fondamentali delle comunicazioni analogiche;

– il consenso è estremamente improbabile che costituisca una base giuridica per il trattamento dei dati personali sul posto di lavoro, a meno che i dipendenti possano rifiutare senza subirne conseguenze negative;

– l'esecuzione di un contratto e gli interessi legittimi possono talvolta essere invocati, a condizione che il trattamento sia strettamente necessario per uno scopo legittimo e conforme ai principi di proporzionalità e sussidiarietà;

– i dipendenti dovrebbero ricevere informazioni efficaci sul monitoraggio (geografico, rispettoso della riservatezza delle informazioni personali (data-oriented), o in relazione al tempo) che si svolge;

– qualsiasi trasferimento internazionale dei dati dei dipendenti dovrebbe avvenire solo qualora sia garantito un adeguato livello di protezione.

Viene posta particolare attenzione a quanto potrebbe essere considerato una sorta di monitoraggio a distanza effettuato dal datore di lavoro tramite l'uso delle nuove tecnologie (es. raccolta di dati relativi alla localizzazione WiFi, analisi di metadati che rilevino stile di vita ed abitudini dell'interessato, ecc.). In tale ottica, il WP29 mette in guardia anche dall'eccessivo monitoraggio sui dipendenti, di fatto evidenziando sempre che qualsiasi sia il trattamento effettuato, con qualsiasi tipo di tecnologia, lo stesso dovrebbe essere limitato a quanto effettivamente tali informazioni siano: necessarie, eque, proporzionate e trasparenti. La posizione di subordinazione in capo al dipendente

già di per sé stessa rende l'ottenimento del consenso da parte del datore di lavoro "minata" dal dubbio che da parte del dipendente sia stato vissuto più come un obbligo che una reale consapevole adesione. Peraltro, anche il legittimo interesse da parte del datore di lavoro non potrà essere considerato un'arma vincente sempre e comunque contro lo scudo del dipendente.

m) Diritti fondamentali ed altre raccomandazioni

Gli Stati membri e l'Unione europea sono anche vincolati dalle disposizioni della Convenzione europea per la salvaguardia dei diritti umani e delle libertà fondamentali che trattano in particolare della riservatezza e della libertà; Art. 8: Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza; ed Art. 10: Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni od idee senza ingerenza alcuna da parte delle autorità pubbliche ed indipendentemente dalle frontiere»[148][149][150].

L'European Data Protection Board (EDPB) ha reso note le linee guida 3/2019 del 12 luglio 2019 sul trattamento dei dati personali in merito ai servizi di videosorveglianza, per le quali è tuttora in corso procedura di consultazione pubblica[151]. Innanzitutto, l'EDPB afferma come un titolare del trattamento sia legittimato ad utilizzare sistemi di videosorveglianza per la tutela del proprio patrimonio qualora vi sia un legittimo interesse che non prevalga sui diritti e le liberà fondamentali degli interessati ripresi.

---

148 Cfr. *http://www.taxlawplanet.it/dati-personali-nei-luoghi-di-lavoro-indicazioni-per-datori-di-lavoro/*

149 Cfr. *https://www.etiprivacy.it/dati-personali-nei-luoghi-lavoro-indicazioni-datori-lavoro*: "*Il principio generale di segretezza della corrispondenza copre le comunicazioni sul posto di lavoro, ed in questo ambito si considerano rientranti la posta elettronica ed i files ad essa acclusi. Ancorché il datore di lavoro risulti proprietario dei dispositivi utilizzati dal dipendente ciò non esclude il loro diritto alla segretezza delle loro comunicazioni e della loro corrispondenza nonché a non essere costantemente localizzati. Perciò il trattamento probabilmente risulterà adeguato solo se è strettamente necessario al legittimo interesse del datore di lavoro per scopi legittimi e rispettosi dei principi di sussidiarietà e proporzionalità (rispetto ai rischi corsi dal datore di lavoro). I datori di lavoro devono inoltre prendere sempre in considerazione il principio di minimizzazione dei dati al momento di decidere sulla implementazione di nuove tecnologie: le informazioni dovrebbero essere conservate per il tempo necessario, con un periodo di conservazione specificato*".

150 Si veda *inter multos* D. LESCE, V. DE LUCIA E P. LONIGRO, *Privacy e rapporto di lavoro. Le linee guida dei Garanti europei* in *diritto24.ilsole24ore.com*, 28 luglio 2017: Il parere, inoltre, ricorda ai datori di lavoro di adottare sempre, nel rispetto del principio di "*accountability*" previsto dal GDPR, misure preventive volte alla protezione della riservatezza dei lavoratori redigendo, se del caso, anche una valutazione di impatto del trattamento che abbia ad oggetto il bilanciamento tra il proprio legittimo interesse e l'impatto delle nuove tecnologie informatiche utilizzate sui diritti e le libertà fondamentali degli interessati.

151 *Guidelines 3/2019 on the processing of personal data through video devices*, op. cit., pag. 1 e ss.

Pertanto, ogni titolare del trattamento dovrà effettuare un bilanciamento di interessi e, qualora il sistema installato sia eccessivamente invasivo nei confronti dell'interessato, dovrà apportare le opportune modifiche volte alla minimizzazione del trattamento. Le linee guida si soffermano anche sul potenziale trattamento di categorie di dati personali derivante da riprese video; in tal senso, è interessante notare l'EDPB coglie anche l'occasione per fornire ulteriori indicazioni sul trattamento di dati biometrici strettamente correlati con i sistemi di videosorveglianza. Dal punto di vista tecnico, il Board afferma come il sistema di videosorveglianza debba essere progettato nel pieno rispetto dei principi di privacy by design e default, limitando le funzionalità del sistema a sole quelle strettamente necessarie alle finalità perseguite e limitando altresì l'accesso alle riprese video a personale qualificato e nominato. Viene ribadita la necessità di effettuare un Data Protection Impact Assessment (DPIA) qualora il Titolare effettui un trattamento di dati personali attraverso un sistema di videosorveglianza»[152]. Ed ancora: «Il testo illustra anche i casi in cui il GDPR non si deve applicare, ad esempio non si applica alle telecamere finte, poiché ogni telecamera non funzionante non tratta dati personali»[153]. «Il bilanciamento degli interessi è obbligatorio. È necessario equilibrare il rapporto tra i "diritti e le libertà fondamentali" da un lato, e i legittimi interessi del titolare dall'altro[154]. Il titolare del trattamento deve sempre valutare attentamente (Considerando 47 del GDPR) i rischi di intrusione sui diritti e le libertà dell'interes-

[152]Cfr. *http://www.avvera.it/prime-considerazioni-sulle-linee-guida-emanate-dallepdb-sui-sistemi-di-videosorveglianza/*

[153] Cfr. *https://www.aips.it/edbp_lineeguida*: "*Le linee-guida riguardano sia i dispositivi video tradizionali sia i dispositivi video intelligenti. Altre tematiche affrontate nel documento, riguardano, tra l'altro: la liceità del trattamento; l'applicabilità dei criteri di esclusione relativi ai trattamenti in ambito domestico; la divulgazione di filmati a terzi. Le linee guida hanno l'obiettivo di fornire gli strumenti utili per evitare che la legittima acquisizione di video registrazioni determini un trattamento illecito dei dati o non conforme al GDPR, ricordando anche che le finalità possono cambiare, a seconda che il titolare sia pubblico o privato, che la videosorveglianza abbia come fine quello di migliorare la sicurezza o di fornire strumenti di pubblicità mirata. Nella parte iniziale del documento si fa accenno anche all'incremento dei rischi del "secondary use" dei dati, generati da sistemi sempre più innovativi dal punto di vista tecnologico e a quelli correlati a un loro eventuale malfunzionamento. è stata fatta quindi anche una distinzione tra tecnologie biometriche complesse e semplici algoritmi di conteggio delle persone in un locale. Su questo punto l'EDPB fa osservare come gli algoritmi non siano sempre del tutto affidabili e indica come i titolari e responsabili dei sistemi di videosorveglianza siano tenuti a mantenere un grado minimo di affidabilità di questi sistemi, per evitare che scelte giuridiche ad essi affidate, come l'identificazione facciale o il riconoscimento, abbiano risultati errati*".

[154] *Guidelines 3/2019 on the processing of personal data through video devices*, op. cit., pag. 3 e ss. "*Ad esempio, nella maggior parte dei casi un dipendente sul posto di lavoro non si aspetta di essere monitorato dal suo datore di lavoro. Allo stesso modo, non è ragionevole attendersi un monitoraggio nei bagni o nelle saune, poiché vi è un intenso "via-vai" di molteplici interessati, nonché per questioni relative all'intimità delle persone. Tuttavia, è sempre necessario valutare caso per caso*".

sato. L'intensità può essere circoscritta, tra l'altro, dal tipo di informazioni raccolte (contenuto delle informazioni), dalla portata (numero delle informazioni, estensione territoriale e geografica), dal numero di persone interessate, dalla situazione in questione, dagli interessi delle persone interessate, da modalità alternative, nonché dalla natura e dalla portata della valutazione dei dati. Per quanto riguarda il "controllo sistematico su larga scala", il rapporto tra l'interessato e il titolare del trattamento può variare significativamente e può incidere sulle ragionevoli aspettative dell'interessato. L'interpretazione del concetto di "*ragionevole aspettativa*" è un criterio molto importante.

Diversamente dal legittimo interesse, il consenso si pone come una base giuridica "*residuale*" in materia di videosorveglianza. Per quanto riguarda il monitoraggio sistematico "*su larga scala*", il consenso dell'interessato può servire da base giuridica ai sensi dell'articolo 7 del GDPR solo in casi eccezionali. Difficilmente il titolare del trattamento sarà in grado di dimostrare che l'interessato ha prestato il proprio consenso prima dell'inizio del trattamento dei dati personali. Inoltre, nel caso dell'esercizio della revoca del consenso, sarà difficile per il titolare del trattamento dimostrare che i dati personali non sono più trattati. In ogni caso, se il titolare del trattamento intende avvalersi del consenso, è suo dovere assicurarsi che ogni interessato che entra nell'area sottoposta a videosorveglianza abbia prestato la sua "*manifestazione di volontà*" cui all'Art. 7 del GDPR[155].

In ottemperanza al principio di minimizzazione dei dati (Art. 5.1 lett. c del GDPR), ed al principio di limitazione della conservazione (Art. 5.1 lett. e del GDPR), i dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali i dati personali sono raccolti e trattati[156].

155 *Guidelines 3/2019 on the processing of personal data through video devices*, op. cit., pag. 3 e ss. "*L'ingresso in un'area con cartello "area videosorvegliata" non costituisce una manifestazione di volontà valida, a meno che non soddisfi i criteri di cui alle Linee Guida WP 259. Inoltre, in ambito lavorativo dato lo squilibrio di potere tra datori di lavoro e dipendenti, nella maggior parte dei casi gli stessi datori di lavoro non possono fare affidamento sul consenso, in quanto è improbabile che venga prestato liberamente dai lavoratori*".

156 *Guidelines 3/2019 on the processing of personal data through video devices*, op. cit., pag. 3 e ss. "*In ogni caso il Comitato sottolinea che in alcuni Stati Membri dell'Unione Europea possono essere previste disposizioni ulteriori a quelle presenti nelle Linee Guida 3/2019 in oggetto. Di solito, afferma il Comitato, i danni che si sono verificati possono essere riconosciuti entro uno o due giorni. Passato questo periodo si procede alla loro cancellazione (solitamente, mediante sovrascrittura automatica). In ogni caso, più lungo è il periodo di conservazione (in particolare quando supera le 72 ore), più argomentazioni bisogna produrre e documentare a sostegno della legittimità della conservazione dei dati (principio di responsabilizzazione, Art. 5.2 del GDPR)*".

In base all'Art. 32 del GDPR, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Il trattamento dei dati personali mediante videosorveglianza non deve essere soltanto legalmente ammissibile, ma anche "*adeguatamente sicuro*". Il sistema di videosorveglianza è costituito nelle seguenti categorie:

- ambiente video: acquisizione delle immagini, interconnessioni e gestione delle immagini.
- lo scopo della cattura delle immagini è la generazione di un'immagine del mondo reale in un formato tale da poter essere utilizzata dal sistema di videosorveglianza;
- le interconnessioni descrivono tutte le trasmissioni di dati all'interno dell'ambiente video (connessioni e comunicazioni);
- la gestione delle immagini include l'analisi, la memorizzazione e la presentazione di un'immagine o di una sequenza di immagini;
- dal punto di vista della gestione del sistema, un sistema di videosorveglianza possiede le seguenti funzioni logiche;
- data management e activity management, che comprendono la gestione dei comandi dell'operatore e delle attività generate dal sistema (procedure di allarme, avviso degli operatori);
- le interfacce con altri sistemi possono includere il collegamento ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) e di altri sistemi che non riguardano la sicurezza (sistemi di gestione degli edifici, riconoscimento automatico delle targhe);
- la sicurezza di un sistema di videosorveglianza consiste nella riservatezza, nell'integrità e nella disponibilità;
- la sicurezza del sistema include la sicurezza fisica di tutti i componenti del sistema e il controllo degli accessi al sistema di videosorveglianza;

- la sicurezza dei dati comprende la prevenzione della perdita dei dati, ovvero la loro manipolazione[157].

4. Conclusioni

Alla luce di tutto quanto sopra esposto[158], l'installazione di un impianto di videosorveglianza "semplice", il cui raggio di rilevamento dei dati copra esclusivamente l'area interessata e, per ovvie e "fisiologiche" ragioni, anche quella immediatamente attigua alle pertinenze aziendali (*id est* zona antistante i cancelli di entrata), non richiede una previa istanza all'Autorità, né specifica notificazione al Garante, sempre che alla stessa (installazione) non si associ una conservazione dei dati registrati superiore ai termini legislativamente previsti (24 ore o, se del caso, una settimana). In tal caso sarà necessario predisporre una relazione che motivi le esigenze di allungamento dei termini di conservazione o addirittura procedere ad una consultazione preventiva dell'Autorità ex art. 36 del GDPR, che si discosta per ratio e modalità di svolgimento dalla verifica preliminare prevista dal vecchio Codice privacy. Altresì, non dovrebbe necessitare il consenso degli interessati. Diversamente, «*nel caso in cui il datore di lavoro intendesse procedere alla predisposizione di sistemi di rilevamento – [per] esigenze di sicurezza sul lavoro – integra [la] fattispecie astratta del c.d. controllo preterintenzionale soggetta a particolari cautele. Di conseguenza, la procedura è più complessa: dovrebbe, dapprima, procedere alla conclusione di un accordo con le rappresentanze sindacali aziendali, ovvero con la commissione interna; ove ciò non fosse possibile, inoltrare un'espressa richiesta di autorizzazione alla Direzione provinciale del lavoro. Dovrebbe, in ogni caso, essere assolto il dovere di informativa, mediante l'affissione del cartello ut supra e la predisposizione di un modello riportante il testo completo messo a disposizione degli interessati. Devono essere nominate per iscritto quali incaricati del trattamento le persone fisiche autorizzate ad accedere ai locali dove sono situate le postazioni di controllo, le persone fisiche che possono utilizzare gli*

[157] Cfr. *https://www.privacy365.it/blog/2019/07/15/i-consigli-e-gli-esempi-nelle-linee-guida-edpb-videosorveglianza-e-gdpr*: «*Come stabilito dall'Art. 25 del GDPR, i titolari del trattamento devono attuare misure tecniche e organizzative adeguate in materia di protezione dei dati prima dell'installazione di un sistema di videosorveglianza (by design), ossia prima di iniziare la raccolta e l'elaborazione dei dati mediante le telecamere, utilizzando per impostazione predefinita i soli dati necessari per le finalità del trattamento (by default)* ».

[158] Cfr, *https://www.altalex.com/documents/news/2016/12/13/videosorveglianza-geolocalizzazione-e-tutela-della-privacy*: «*Come noto, il Regolamento (UE) n. 2016/679 ha introdotto diverse novità in materia di data protection. Anche la disciplina interna delle attività di videosorveglianza, dunque, dovrà adeguarsi alla normativa europea a far data dal 25 maggio 2018*».

impianti di videosorveglianza, nonché quelle autorizzate a visionare le immagini. Infine, devono adottarsi le opportune misure di sicurezza riportate anche nel Registro dei trattamenti»[159].

[159]Cfr. *https://www.altalex.com/documents/news/2016/12/13/videosorveglianza-geolocalizzazione-e-tutela-della-privacy*

PRIVACY: UTILIZZO DEI SOCIAL NETWORK DURANTE L'ORARIO LAVORATIVO

di Francesco Lo Chiatto

SOMMARIO. 1. Premessa. 2. Linee guida del Garante, n. 58 del 10 marzo 2007. 3. Come si sono espressi nel merito: Cassazione e Tribunali locali in Italia. 4. Sentenza Cedu 17 ottobre 2019. 5. Conclusioni.

This work, starting from a discussion on the use of social networks, focuses in particular on the use of these tools, during working hours. In this regard, it was important to dwell on the Guidelines of the Privacy Guarantor n.58 of 2007, which carefully and precisely focus on the relationship between employer and worker and the privacy of the latter, in order to protect it by implementing preventive and never successive and invasive tools of the private sphere. The ordinary work performed by the various courts and the Court of Cassation is also fundamental, as they resolve problems and issues, which move borderline between the rights of the employer and the rights of the worker. Finally, a careful look was given to the last sentence of the ECHR, which in October 2019, confirming the ruling of the local Spanish court, giving reason to the employer, specified that only in extrema ratio and when there are specific founded reasons is it possible to override the employee's privacy, but for a very limited and extremely long period without any diffusion of this. With a note, the Privacy Guarantor specified that this sentence affirms the principles of Gdpr 679/2016, which sees the principle of relevance and not excess as a fundamental element for the protection of privacy.

1. Premessa

La tecnologia negli ultimi anni ha fatto passi da gigante, al punto che il modo di comunicare con le persone cambia di anno in anno. Lontani ormai i tempi delle lettere e dei telefoni fissi, si è approdati nell'era dei social network, attraverso i quali avvengono gran parte delle comunicazioni. È evidente come i social network facciano sempre più parte della nostra vita, in quanto in tempo reale, ci permettono di conoscere notizie, pubblicare istantanee e comunicare e condividere con amici e non, messaggi o foto in tempo reale, ma anche condividere curriculum e candidature. Tra i social più

noti ricordiamo *Facebook, Instagram, WhatsApp, Linkedin*, Twitter. Una domanda lecita, visto l'uso quotidiano di questi social, è quella relativa all'utilizzo degli stessi durante l'orario lavorativo. In un'ottica di bilanciamento di interessi è rilevante tutelare, sia il datore di lavoro, affinché possa controllare che non vi sia un assenteismo virtuale del lavoratore, sia il lavoratore, che non veda violata la sua privacy. Uno sguardo ad un messaggio o qualche secondo di distrazione non può considerarsi un comportamento perseguibile, soprattutto se accade *una tantum*. La questione è quando questa distrazione risulta prolungata ed avviene quotidianamente. Il problema che va rilevato non è l'utilizzo del pc aziendale per andare sui social network, lo stesso varrebbe se fosse utilizzato il proprio dispositivo personale, bensì il tempo lavorativo che viene sottratto all'azienda. Per contrastare l'utilizzo dei social, da parte dei propri dipendenti, il datore di lavoro può inibire l'accesso agli stessi con un filtro preventivo sul server aziendale, oppure optare secondo un criterio di ragionevolezza, lasciando l'accesso ai social in alcuni momenti della giornata lavorativa, come la pausa pranzo. Tuttavia, l'azienda che decida di effettuare i controlli sulla navigazione internet dei propri dipendenti, dovrà rispettare alcune regole definite nelle "*Linee Guida per la posta elettronica e internet*" emanate dal Garante per la privacy. È previsto, infatti, che i datori di lavoro informino i lavoratori sulle modalità di utilizzo di Internet e della posta elettronica e sulla possibilità che vengano effettuati controlli.[160]

2. Linee guida del Garante, n. 58 del 10 marzo 2007

A tale proposito risulta utile e opportuno soffermarsi sulle linee guida del Garante, n.58 del 10 marzo 2007, relativamente a posta elettronica ed internet nel rapporto di lavoro.

Negli anni è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato, per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet. L'utilizzo di Internet e parimenti della posta elettronica, potrebbe portare nel caso di mancanza di cautele e misure di sicurezza, ad analisi, profilazione e ricostruzione integrale di log file della navigazione web e log-file di traffico e-mail, facendo conoscere al datore di lavoro il contenuto della corrispondenza. Le informazioni eventualmente assunte porterebbero a un trattamento di dati

[160] Cfr. *http://www.casigliaronzoni.it/laccesso-ai-social-network-da-parte-dei-dipendenti/*

personali e sensibili, riguardanti il lavoratore o terzi, identificati o identificabili. Il luogo di lavoro, infatti, è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l´esplicazione della personalità del lavoratore, insieme a una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (*artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l´art. 2, comma 5, Codice dell´amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche, sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato*. Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, dei principi di semplificazione, armonizzazione ed efficacia. Alcune disposizioni di settore prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza, *artt. 4 e 8 l. 20 maggio 1970, n. 300*. I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell´osservanza di alcuni cogenti principi, quali il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l´utilizzazione di dati personali e di dati identificativi, in relazione alle finalità perseguite e il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all´attività lavorativa e quindi i trattamenti devono essere effettuati per finalità *determinate, esplicite* e *legittime* osservando il principio di *pertinenza* e *non eccedenza*. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*, infatti le attività di monitoraggio devono essere svolte solo da soggetti preposti e devono essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"*. In base, al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore all'*art. 4, secondo comma, Statuto dei lavoratori.* Grava, quindi, sul datore di lavoro l´onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti che ha disposizione e se, e in che misura e con quali modalità vengano effettuati eventuali controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali. In questo

quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente, verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall´art. 7 dello Statuto dei lavoratori, e da sottoporre ad aggiornamento periodico. All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell´art. 13 del Regolamento 2016/679. Rispetto a eventuali controlli, gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli. Devono essere tra l'altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l'unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti. Il datore di lavoro può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (*cfr. artt. 2086, 2087 e 2104 cod. civ.*). Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (*art. 4, primo comma, l. n. 300/1970*), tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica. Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa, ciò anche quando i singoli lavoratori ne siano consapevoli. In particolare, non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l'attività di lavoratori, come la lettura e la registrazione sistematica dei messaggi di posta elettronica, la riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore. Secondo il principio di necessità, il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e infatti ha l´onere di adottare tutte le misure *tecnologiche* volte a minimizzare l´uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet, consistenti in attività non correlate alla prestazione lavorativa, quali la visione di siti non pertinenti, l'upload o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all´attività, deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore.

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i *file* allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali. Un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (*artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale*). Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica per uso personale pur operando in una struttura lavorativa. La mancata esplicitazione di una *policy* al riguardo, può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest'ultimo (posta "in uscita"). Risulta opportuno a tal punto, che il datore di lavoro doti il lavoratore, di indirizzi di posta elettronica condivisa, o un indirizzo di posta elettronica, e metta a disposizione di ciascun di esso apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze, come per ferie o attività di lavoro fuori sede, messaggi di risposta contenenti le "coordinate" di un altro soggetto o altre utili modalità di contatto della struttura, tali da prevenire l´apertura della posta elettronica. In caso di eventuali assenze non programmate come per malattia, qualora il lavoratore non possa attivare la procedura descritta, il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato, come l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati, l´attivazione di un analogo accorgimento, avvertendo gli interessati. In previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato deve essere messo in grado di delegare un altro lavoratore, il fiduciario, al fine di verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il

lavoratore interessato alla prima occasione utile. Ulteriore sistema a tutela del lavoratore devono essere i sistemi *software* programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non risulti necessaria. [161]

3. Come si sono espressi nel merito: Cassazione e Tribunali locali in Italia.

Dopo un'attenta analisi di tutte quelle che sono le disposizioni che vanno a bilanciare gli interessi delle due categorie, risulta interessante dare uno sguardo veloce alla giurisprudenza italiana, che ben si è espressa nei differenti casi, per poi passare ad analizzare la recentissima sentenza della Corte di Strasburgo, che pone alcuni principi fondamentali, per meglio bilanciare gli interessi delle varie categorie. A tale proposito risulta utile richiamare la sentenza n.3133/2019 emanata dalla Corte di Cassazione, che ha confermato le precedenti decisioni del Tribunale di Brescia (sentenza 13 giugno 2016, n.782 e della corte di Appello di Brescia, che avevano dichiarato legittimo il licenziamento di una impiegata part time, che nell'arco di soli 18 mesi aveva effettuato circa 6.000 accessi ad internet estranei all'ambito lavorativo di cui almeno 4.500 circa sul suo profilo personale Facebook. Questa sentenza sembra proseguire il lavoro gia iniziato in altri tribunali, come quello di Milano, che ha rigettato il ricorso di un dipendente licenziato per avere illegittimamente utilizzato Facebook ed internet sul luogo di lavoro, facendo foto nell'azienda e pubblicandole su facebbok condendola con frasi altamente offensive contro il datore di lavoro, oltre ad aver avuto accesso più volte durante l'orario lavoro a siti di carattere pornografico (Trib. Milano ordinanza 1 agosto 2014 nella causa r.g. n. 6847/2014). Anche la Cassazione, in più occasioni, ha ribadito come il continuo accesso ad Internet o alla propria pagina personale Facebook possa giustificare la sanzione espulsiva da parte del datore di lavoro e, infatti, è stato dichiarato legittimo il licenziamento di un dipendente che si era connesso per fini personali ad internet per 27 volte nell'arco di due mesi, restando collegato per 45 ore complessive (Cass 13 giugno 2017, n. 14862), cosi come quando il datore di lavoro abbia il sospetto che il suo dipendente abusi degli strumenti informatici messigli a disposizione per intrattenere lunghe conversazioni su Facebook, può ben creare un falso profilo di donna con il quale attirare il lavoratore e così provare lo svolgimento di attività ludica durante l'orario di lavoro (Cass. 27 maggio 2015, n. 10955). In senso opposto a tali

[161] Cfr. *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522*

sentenze, si è invece espresso il Tribunale di Firenze che ha ritenuto illegittimo il licenziamento irrogato nei confronti di un dipendente che su 163 giorni nei quali ha effettuato almeno un collegamento a internet in orario di lavoro, ha dedicato a tale attività mediamente circa 56 minuti giornalieri (Trib. Firenze 7 gennaio 2008, n. 1218). In tal caso, il licenziamento è stato annullato anche sul presupposto che il datore di lavoro aveva sempre consentito un accesso alla rete internet per motivi extra lavorativi, sia pure nei limiti della ragionevolezza e purché il sistema non fosse tenuto occupato per tempi eccessivi. Anche per Cass. 2 novembre 2015, n. 22353, è illegittimo il licenziamento per giusta causa di un lavoratore per uso illegittimo del PC aziendale, delle reti informatiche aziendali e della casella di posta elettronica, se il datore di lavoro non prova un danno ulteriore e infatti nello specifico, non era risultato in giudizio che la navigazione in internet del dipendente avesse determinato una significativa sottrazione di tempo all'attività di lavoro. L'utilizzo di Facebook o di internet può comportare conseguenze negative per il lavoratore, non soltanto quando avvenga durante l'orario di lavoro, ma anche fuori da tale ambito, soprattutto ove si configuri un danno all'immagine del datore di lavoro o una vera e propria diffamazione, penalmente perseguibile. Infatti, secondo la Suprema Corte, la diffusione di un messaggio offensivo attraverso l'uso di Facebook assume valenza diffamatoria per la potenziale capacità di raggiungere un numero indeterminato di persone e, di conseguenza, integra giusta causa di licenziamento (Cass. 27 aprile 2018, n. 10280).[162]

4. Sentenza Cedu 17 ottobre 2019

Il caso all'origine della Sentenza Cedu (sentenza 17 ottobre 2019 sui ricorsi 1874/13 e 8567/13) risale al 2009, quando il direttore di un supermercato spagnolo in provincia di Barcellona, rilevando irregolarità tra stock di magazzino e vendite, aveva verificato un'ingente perdita negli incassi nell'arco di cinque mesi, di circa 82.000 euro. Alla luce di ciò, ha deciso di far installare alcune telecamere a circuito chiuso, visibili alle uscite e nascoste sulle casse. Le videoriprese hanno evidenziato una serie di furti di merci da parte del personale, al quale sono seguite 14 lettere di licenziamento per motivi disciplinari tra cassieri e addetti alle vendite. Nonostante i licenziamenti siano stati

[162] Cfr. *http://www.quotidianogiuridico.it/documents/2019/03/04/utilizzo-di-internet-e-facebook-sul-luogo-di-lavoro-per-fini-extra-lavorativi*

considerati legittimi dai tribunali nazionali, cinque dipendenti allontanati, hanno deciso di ricorrere alla Corte di Strasburgo. In base al diritto spagnolo i cassieri dovevano essere preventivamente informati della sorveglianza e oltre questo si chiedeva alla Corte l'applicazione dell'art.8 della Convenzione europea dei diritti dell'uomo, che riguarda la sfera della vita privata e familiare, che in questo caso secondo loro sarebbe stata violata. Per i giudici della Corte Europea, (14 voti favorevoli e tre contrari), i tribunali nazionali spagnoli avevano attentamente bilanciato i diritti dei dipendenti sospettati di furto e quelli del datore di lavoro, effettuando un esame approfondito delle ragioni della videosorveglianza. La mancata notifica che è stata oggetto della contestata contesa, così come prevista anche dalle norme iberiche, in questo caso troverebbe una deroga al principio applicativo, in quanto il tutto sarebbe giustificato da un "ragionevole sospetto" di una grave colpa dei cassieri e dall'entità della perdita economica subita dal supermercato a causa dei furti. Nel ritenere il monitoraggio "proporzionato e legittimo" e l'intrusione nella privacy dei ricorrenti non eccessivamente grave, i giudici spagnoli non hanno quindi superato il loro potere discrezionale ("margine di apprezzamento") anche per la sua breve durata, all'incirca dieci giorni, e per il numero limitato di persone messe a conoscenza dei video. È risultata fondamentale, anche la scarsa estensione dell'area sorvegliata, limitata alla sola zona casse. Per la Cedu il livello di privacy che un dipendente può legittimamente attendersi, dipende infatti, anche dalla posizione, molto elevato in luoghi privati, come servizi igienici o guardaroba, dove vi è un divieto assoluto di videosorveglianza, elevato in spazi di lavoro ristretti come gli uffici, dove può essere giustificato e inferiore negli spazi di lavoro visibili o accessibili ai colleghi o al pubblico in generale. La linea della Cedu è condivisa dal Garante privacy italiano, che in una nota ha sottolineato come la sentenza da una parte giustifica, nel caso di specie le telecamere nascoste, dall'altra conferma però il principio di proporzionalità come requisito essenziale di legittimazione dei controlli in ambito lavorativo. Per il via libera alla videosorveglianza "segreta" la Corte di Strasburgo ha infatti accertato una serie di presupposti, come "i fondati e ragionevoli sospetti" sui furti commessi dai lavoratori e il danno ingente subito dal datore di lavoro. Il Garante ha commentato che la videosorveglianza occulta è ammessa solo in quanto *extrema ratio*, con modalità spazio-temporali tali da limitare al massimo l'incidenza del controllo sul lavoratore, e in alcun modo può divenire prassi ordinaria. Il Garante ha concluso dicendo che i requisiti legittimi per i controlli sul lavoro, devono rispettare

i principi di proporzionalità e di non eccedenza, che risultano i capisaldi della protezione dei dati personali. [163]

5. Conclusioni.

A conclusione del presente lavoro, si evince come il progresso abbia fatto passi da gigante anche nel campo delle comunicazioni, interessando la nostra quotidianità in maniera capillare. È nell'ambito lavorativo, che si creano problemi propri e impropri, tra datore di lavoro e dipendenti. Spesso può accadere che un datore di lavoro, per verificare se si è in presenza di un eventuale assenteismo virtuale, possa prevaricare la privacy del proprio dipendente, con controlli inopportuni. Fondamentali a questo punto sono stati i riferimenti dapprima alle linee Guida del Garante, che hanno creato la linea di demarcazione tra i controlli del lavoratore e il diritto alla privacy del dipendente, attraverso strumenti preventivi e mai successivi e invasivi della sfera di quest'ultimo. In tal senso, determinanti risultano i richiami alle sentenze dei vari tribunali locali e della Cassazione, che si sono espressi in maniera alterna a favore di uno o dell'altro, a seconda dei casi. In ultimo è stato rilevante leggere la sentenza della Cedu, emanata nell'ottobre 2019, in cui è stata confermata la sentenza del tribunale locale spagnolo, che dava ragione al datore di lavoro, che aveva controllato alcuni dipendenti con telecamere nascoste. Tale caso, anche se potrebbe far pensare a una violazione della privacy dei dipendenti, risulta una *extrema ratio*, giustificata da fondati motivi, tempo minimo di controllo e nessuna diffusione di tali immagini. Lo stesso Garante Privacy italiano, si è unito favorevolmente all'espressione di tale sentenza, in quanto ripercorre e richiama il principio fondamentale, previsto all' interno del GDPR, che è quello della pertinenza e non dell'eccedenza.

[163] Cfr. *https://www.ilsole24ore.com/art/cedu-furti-ingenti-e-ragionevoli-sospetti-legittimano-telecamere-nascoste-luogo-lavoro-ACiJ3ks*

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*