Corrado Cardarello – Gabriele Lipari

La privacy ed il rapporto di lavoro subordinato

Giappichelli

PREMESSA

Come ho sostenuto in alcuni convegni, solo ad una analisi superficiale la normativa del GDPR, ovvero del Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, può apparire complessa e/o farraginosa.

A ben vedere, al contrario, si tratta di un impianto normativo completo ed evoluto che sposta il baricentro della tutela da un piano remediale e repressivo ad uno di natura squisitamente preventiva.

In verità è molto agevole comprendere la normativa in questione e coglierne il profondo significato innovativo se si approccia la lettura del GDPR in modo strutturato, ovvero rispondendo a talune domande chiave.

Ovviamente sarebbe arduo, se non persino presuntuoso, pretendere di riassumere in poche righe tutta la normativa afferente il GDPR.

Nondimeno, a mo' di drone che sorvola un territorio, appare utile fornire una visione di insieme dei punti fondamentali del GDPR per comprendere meglio come e quanto il tema della tutela dei dati personali sia fondamentale nel rapporto di lavoro subordinato, aspetto che costituisce appunto l'oggetto della presente opera.

Per rispondere quindi alle domande chiave, occorre dunque percorrere il sentiero dell'analisi mediante passi logici e successivi.

* * *

La premessa di base è che, ai sensi dell'art. 1, il Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

* * *

Il primo *step* consiste dunque nell'interrogarsi sulla finalità della normativa.

Ovvero occorre chiedersi quale sia il "bene" tutelato.

È sufficiente evidenziare che la *privacy* oggi non si configura più come *the right to be let alone,* ovvero come "*il diritto di essere lasciato solo*", secondo una corrente di pensiero degli anni '70 che valorizzava il solipsismo quale protocellula della condizione umana.

Oggi la *privacy*, più correttamente la *data protection*, può ben essere definita come un diritto fondamentale ed inviolabile, come peraltro esplicitato nel Considerando 1 del GDPR.

Ovvero come il diritto dell'individuo – definito "interessato" dalla norma – a controllare i propri dati e la destinazione e diffusione che essi ricevono sulla base della valorizzazione massima del consenso dell'individuo stesso.

Invero nel Considerando 7 si legge che "*... è opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche ...*".

Inviolabilità e consensualità ovviamente non sono sinonimi di illimitatezza della tutela.

Invero tale diritto ben può ricevere delle compressioni laddove sussistano interessi di altri soggetti meritevoli pure di tutela, oppure finalità di interesse pubblico ed ultraindividuale che trascendono la sfera del singolo, come nel caso di esigenze di sicurezza, salute, ricerca scientifica, analisi statistica, ecc.

Non a caso nel Considerando 4 al Regolamento si legge che "*... Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità ...*".

Quindi una prospettiva ed un perimetro affatto diversi e molto più ampi ed articolati rispetto al passato ed al "*diritto di essere lasciato solo*".

A ciò si deve aggiungere una ulteriore e nodale riflessione per cui il dato personale è oramai assurto a valore economico, propulsore della economia basata sui *big data* e straordinario volano del *business*.

Tale presa d'atto, anche in una visione prospettica, è rinvenibile nel Considerando 13 al GDPR ove possiamo leggere: "*Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei di-*

versi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

In altri termini, la *data protection* è un diritto fondamentale dell'individuo che deve essere protetto e tutelato, anche nei suoi risvolti economici, nell'ambito di una cornice normativa di certezza delle tutele poste a presidio della sua libera circolazione.

* * *

Peraltro, il nostro percorso presuppone che si risponda ad un'altra domanda chiave.

Ovvero è necessario chiedersi "chi" sia il soggetto destinatario della tutela approntata dalla normativa.

Su questo tema non vi sono particolari dubbi, al massimo possono sussistere zone di confine.

Il destinatario è soltanto "l'interessato", come accennato in precedenza, che coincide con la persona fisica, ovvero il soggetto che acquista la capacità giuridica dal momento della nascita *ex* art. 1 c.c. e la conserva fino al momento della morte.

Ne consegue come primo corollario che sono esclusi dall'ambito di applicazione della norma le persone giuridiche e, in generale, tutti i soggetti per i quali non sia sotteso un substrato corporeo.

Infatti, il Considerando 14 recita che il Regolamento non disciplina il trattamento dei dati personali delle persone giuridiche, in particolare delle imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica ed i suoi dati di contatto.

Dunque, mentre non vi sono dubbi sull'applicazione della normativa al lavoratore subordinato, per come definito dall'art. 2094 c.c., ben difficilmente potrebbe invocare detta applicazione un CRAL – un circolo ricreativo aziendale dei lavoratori – che si configurasse come associazione non riconosciuta e portatrice di diritti non riferibili ai singoli dipendenti (e solo da essi esercitabili).

Ragionando negli stessi termini non appare applicabile la normativa alle organizzazioni sindacali dei lavoratori in quanto associazioni non riconosciute a meno che non sia tutelata la posizione di un singolo iscritto.

Infatti il Considerando 142 del Regolamento prevede che "*Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del presente Regolamento, dovrebbe avere il diritto di dare mandato ad un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro ...*

per proporre reclamo per suo conto ad un'autorità di controllo, esercitare il diritto ad un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati ...".

Quanto detto in ordine alla esclusiva riferibilità alla persona fisica della tutela non esclude tuttavia che in alcuni casi la tutela del GDPR sia invocabile, in ipotesi dalla persona fisica titolare della ditta individuale la cui denominazione coincida con le generalità della suddetta persona fisica o laddove il profilo della persona fisica assuma una connotazione dominante nell'ambito della fattispecie concreta.

Inoltre, il requisito della vitalità non impedisce che vi siano situazioni meritevoli di tutela anche *post mortem*.

Si pensi alla situazione della cessazione del rapporto di lavoro per causa di morte, alla liquidazione delle competenze di fine rapporto ed ai diritti degli aventi causa, sia per successione *ab intestato* o testamentaria, sia *iure proprio.*

Invero non è raro che il datore di lavoro, secondo lo schema del contratto a favore di terzo, sostenga l'onere del premio assicurativo per il dipendente in relazione ad una polizza vita con indennizzo economico i cui destinatari sono liberamente designati dal *de cuius* a prescindere dalle disposizioni codicistiche sulla quota di riserva e sui soggetti successibili *ex lege.*

Sul punto soccorre l'art. 2-*terdecies* del Codice della Privacy, ovvero del d.lgs. n. 196/2003, modificato dal d.lgs. n. 101/2018.

Per inciso val bene ricordare che, pur ritenendo opportuno assicurare un'applicazione coerente e omogenea delle norme in tutta l'Unione, il Considerando 10 prevede che il GDPR non esclude che il diritto degli Stati Membri, come nel caso del d.lgs. n. 196/2003, stabilisca le condizioni per specifiche situazioni di trattamento.

Quindi detto articolo prevede che "*... i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione. ... La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera ed informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma. ... In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi ...*".

* * *

Delineati quindi gli elementi afferenti alle finalità della normativa ed il soggetto protetto dalle norme si impone anche l'analisi di un ulteriore profilo, ovvero "il cosa", che, peraltro, è strettamente correlato al "chi".

E qui sovviene il concetto di "dato personale".

Per dato personale deve intendersi qualsiasi elemento che, essendo astrattamente inerente all'interessato o essendo a lui riconducibile, lo identifica o lo rende identificabile, tale quindi da determinare il diritto dell'interessato al controllo in ordine all'utilizzo che altri possono fare dei suoi dati personali.

Per migliore dettaglio l'art. 4, comma 1, del GDPR, definisce il dato personale "*come qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

Ovviamente tutti i dati personali sono importanti, si pensi alle generalità anagrafiche, alla residenza o al domicilio, al sesso, e così via.

Persino i riferimenti di un conto corrente bancario di recente sono stati considerati "dato personale".

Ma alcuni evidentemente rivestono uno specifico rilievo in quanto la loro conoscenza da parte di terzi può determinare un accentuato livello di invasività della sfera dell'interessato.

E tale rilievo ha appunto ricevuto cittadinanza nel GDPR con la previsione dell'art. 9 il quale recita che "*è vietato trattare dati personali che rivelino l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ...*".

Peraltro, il comma 2 del citato art. 9 specifica che il par. 1 non si applica a vari casi, tra cui, per anticipare subito quelli di maggiore attinenza con l'ambito del rapporto di lavoro, val bene ricordare:

– quando l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati per una o più finalità specifiche;

– se il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

– se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

– se il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

– se il trattamento è necessario per finalità di medicina del lavoro o di valutazione della capacità lavorativa del dipendente.

Val bene evidenziare che i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati (art. 2-*novies* del d.lgs. n. 196/2003).

Ovviamente, in particolare nell'ambito dei rapporti contrattuali, assume dunque fondamentale rilevanza il consenso dell'interessato che deve essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata ed inequivocabile di accettare il "trattamento" dei dati personali che lo riguardano.

Invero, a mente del Considerando 32, "*... Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso ...*").

Evidentemente qualora il "trattamento" abbia più finalità, il consenso deve essere prestato per tutte le suddette finalità.

* * *

A questo punto, focalizzata l'attenzione sulla finalità della normativa, sulla natura del diritto tutelato, sul soggetto protetto, sull'oggetto costituito dai dati personali nonché sul consenso, occorre fare un ulteriore passo decisivo nel nostro sentiero.

Volutamente in precedenza è stato fatto ricorso in modo improprio al termine "utilizzo" dei dati personali.

Se invece seguiamo il percorso della corretta nomenclatura, è assolutamente ortodosso avvalersi del termine "trattamento".

E qui è necessario esaminare la previsione dell'art. 4, comma 2, del GDPR che lo definisce con una puntualità che non lascia spazi ad interpretazioni restrittive od estensive.

Segnatamente il citato articolo qualifica come trattamento "*... qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione ...*".

Quindi la lettura del suddetto articolo ci apre subito la strada ad alcuni punti fermi:

a) non si può parlare di trattamento nel senso previsto dalla normativa se i dati sono anonimi, ovvero se non consentono la identificazione o l'identificabilità dell'interessato, oppure se non riguardano una persona fisica;

b) i dati possono essere trattati solo per finalità determinate e legittime che devono, per lo più, essere portate a conoscenza dell'interessato mediante apposita informativa e previa acquisizione del suo consenso;

c) il consenso deve essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata ed inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale;

d) qualora il trattamento abbia più finalità, il consenso deve essere prestato per tutte queste;

e) ogni trattamento presuppone l'esistenza di uno o più soggetti che utilizzano questi dati a vario titolo e con l'adozione di apposite misure di sicurezza.

Si aggiunga che, in base al Considerando 18 ed all'art. 2, comma 2, lett. c), il Regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale.

Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei *social network* ed attività *on line* intraprese nel quadro di tali attività.

* * *

Allora è arrivato il momento di calarci sempre più nel perimetro della normativa ed analizzare quali sono i soggetti che utilizzano questi dati.

Su questo sovviene ancora il testo normativo con la definizione del "Titolare del trattamento" e del "Responsabile del Trattamento".

Ai sensi dell'art 4, comma 7, del GDPR il Titolare del trattamento è 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.

Quindi, nei casi che ci interesseranno in seguito, il Titolare è il datore di lavoro.

Non sono pochi, e sono assolutamente di rilievo, gli obblighi del Titolare.

Infatti, a titolo esemplificativo, a parte quanto previsto dagli artt. 24 e 25 del Regolamento:

– il Titolare è responsabile per qualsiasi trattamento di dati personali che abbia effettuato direttamente o che altri abbiano effettuato per suo conto (Considerando 74);

– adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli artt. da 15 a 22 e all'art. 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro;

– è tenuto a mettere in atto misure adeguate ed efficaci in grado di dimostrare la conformità delle attività di trattamento con il regolamento, compresa l'efficacia delle misure;

– deve adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita (Considerando 78);

– deve ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse (Considerando 81);

– deve tenere ed aggiornare un registro delle attività di trattamento effettuate sotto la sua responsabilità (Considerando 82);

– deve valutare i rischi inerenti al trattamento ed attuale misure per limitare tali rischi, quali la cifratura (Considerando 83);

– deve svolgere una valutazione di impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio (Considerando 84);

– deve comunicare all'interessato la violazione di dati personali senza indebito ritardo, qualora questa violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie (Considerando 86);

– deve risarcire i danni cagionati ad una persona da un trattamento non conforme al Regolamento, salvo essere esonerato da responsabilità ove di-

mostri che l'evento dannoso non gli è in alcun modo imputabile (Considerando 146).

Inoltre, l'art. 4, comma 8, del GDPR definisce Responsabile del trattamento la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dai personali per conto del titolare del trattamento.

Ancora l'art. 28 del Regolamento precisa che:

– qualora un trattamento debba essere effettuato per conto del Titolare, questi ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate;

– il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare;

– i trattamenti da parte del responsabile sono disciplinati da un contratto o da altro atto giuridico che deve disciplinare la materia, durata, natura e finalità del trattamento, il tipo di dati personali, le categorie di interessati e gli obblighi e i diritti del Titolare.

Dunque, sempre in via esemplificativa, "un Responsabile" può essere il soggetto esterno incaricato dal datore di lavoro/Titolare di gestire il processo relativo alle paghe e contributi dei dipendenti.

* * *

Posto così l'impianto generale, e senza dimenticare istituti e figure non meno importanti che ricorreranno nel corso del presente volume (l'Autorità Garante [1],

[1] Art. 58, *Poteri* (C122, C129): "*1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti: a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti; b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati; c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7; d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento; e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.*

2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del tratta-

il *Data Protection Officer*[2], le norme vincolanti d'impresa o *binding corpo-*

mento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti: a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36; b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali; c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare; d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5; e) accreditare gli organismi di certificazione a norma dell'articolo 43; f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5; g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d); h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b); j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.

4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta.

5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso.

6. Ogni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 2 e 3. L'esercizio di tali poteri non pregiudica l'operatività effettiva del capo VII".

[2] Art. 39, *Compiti del responsabile della protezione dei dati* (C97): "*1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del perso-*

rate rules, il *data breach*, le sanzioni amministrative [3] e quelle penali [4], le linee guida, ecc.), occorre ora pervenire al binomio che caratterizza il trattamento dei dati personali.

Ma prima di far questo, occorre ricordare le previsioni di alcuni articoli fondamentali del GDPR.

Segnatamente l'art. 5 afferma che i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità dei dati

d) esatti e, se necessario, aggiornati, con l'adozione di tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

---

nale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo".

[3] Considerando 150: "*Al fine di rafforzare e armonizzare le sanzioni amministrative applicabili per violazione del presente regolamento, ogni autorità di controllo dovrebbe poter imporre sanzioni amministrative pecuniarie. Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione*".

[4] Considerando 149: "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtu' ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare n la sottrazione dei profitti ottenuti attraverso violazioni del presente Regolamento ...*". Il d.lgs. n. 196/2006 prevede l'art. 167 sul trattamento illecito dei dati, l'art. 167-*bis* sulla comunicazione e diffusione di dati personali oggetto di trattamento su larga scala, l'art. 167-*ter* sulla acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala, l'art. 168 sulla falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante, l'art. 170 sulla inosservanza dei provvedimenti del Garante, l'art. 171 sulle violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori, l'art. 172 sulle pene accessorie.

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche ed organizzativa adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (ovvero dalla comunicazione e dalla diffusione dei dati personali a soggetti diversi dall'interessato).

Questo articolo ci restituisce in ultima analisi la "carta dei doveri" del Titolare/datore di lavoro, che si può riassumere evidenziando i seguenti principi, e che, per converso, costituiscono profili di esigibilità da parte del lavoratore:

– liceità;
– correttezza;
– trasparenza;
– minimizzazione;
– esattezza;
– integrità;
– riservatezza.

Non a caso il comma 2 dell'art. 5 recita che il titolare del trattamento è competente per il rispetto dei principi suindicati e deve essere in grado di comprovarlo secondo quello che in una accezione più ampia può essere definito come il "principio di responsabilizzazione".

Il profilo probatorio, lo si evidenzia subito, è di estrema importanza in quanto, se si ritiene applicabile alla materia l'art. 2050 c.c. [5] relativo alle attività pericolose, l'onere della prova richiede in questo caso la dimostrazione di aver fatto tutto il possibile per evitare un evento.

Restringendo poi l'attenzione all'aspetto negoziale ed al consenso, si evince chiaramente dall'art. 6 del GDPR che il trattamento è lecito, tra i vari casi, solo e se l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, se il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, se il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

Ed in base all'art. 7 del GDPR, qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'in-

[5] Art. 2050 c.c.: "*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*".

teressato ha prestato il proprio consenso al trattamento dei propri dati personali per determinate finalità.

Ne consegue che il binomio che costituisce l'oggetto principale dell'analisi che seguirà è quello che possiamo definire secondo la semplice equazione di cui appresso, ovvero Lavoratore-interessato/datore di lavoro-Titolare del trattamento ed Informativa/consenso/trattamento.

Da ciò deriva, altresì, che questa equazione può connotarsi ulteriormente ed ampliarsi ove il titolare del trattamento faccia parte di un gruppo imprenditoriale o di enti collegati ad un organismo centrale e possa avere un interesse legittimo a trasmettere i dati personali all'interno della realtà più ampia, fosse anche verso un Paese terzo.

Infatti, un gruppo imprenditoriale deve costituirsi di un'impresa controllante e delle sue controllate, laddove l'impresa controllante deve essere quella che può esercitare un'influenza dominante sulle controllate in forza, ad esempio, della proprietà, della partecipazione finanziaria o delle norme societarie o del potere di fare applicare le norme in materia di protezione dei dati personali (Considerando 37).

Peraltro un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti di impresa approvate per i trasferimenti internazionali dall'Unione agli organismi dello stesso gruppo imprenditoriale o gruppo d'imprese che svolge un'attività economica comune, purché tali norme contemplino tutti i principi fondamentali e diritti azionabili che costituiscano adeguate garanzie per i trasferimenti o categorie di trasferimenti di dati personali (Considerando 110).

* * *

In questo *framework* si pongono temi assolutamente non semplici e che in alcuni casi appaiono restituire risposte certe, in altri sono fonte di notevole dibattito, in altri ancora sono persino inesplorati.

Si pensi, per esempio, alla "prova di resistenza" straordinaria che il GDPR e tutti gli addetti ai lavori hanno dovuto fronteggiare con la pandemia e con la recente normativa nazionale sul *Green Pass*, che ha posto interrogativi di enorme rilievo, in particolare nell'ambito del rapporto di lavoro, in termini di compatibilità tra il diritto alla riservatezza e l'esigenza di protezione della salute.

E lo scopo che con il Collega Gabriele Lipari ci siamo riproposti con questa opera è di portare il nostro contributo di esperienza quotidiana di giuslavoristi, nonché di *data protection officers*, per tentare di fornire una mappatura analitica dei temi in discussione.

CORRADO CARDARELLO