Introduzione alle novità normative del Regolamento (UE) 679/2016 sulla protezione dei dati personali

Abstract

Il Regolamento (UE) 2016/679, c.d. Regolamento Generale sulla Protezione dei Dati e noto anche come GDPR, divenuto applicativo lo scorso 25 maggio, introduce importanti novità nel sistema della protezione dei dati personali pur non modificando in modo essenziale l'impianto preesistente. In questo contributo si presenta un'introduzione a tale normativa tentando di delineare il contesto nel quale essa si colloca e i suoi presupposti ideali. Vengono inoltre esposte sinteticamente le più rilevanti novità e individuate alcune questioni rilevanti per il diritto del lavoro. In conclusione si propongono alcune valutazioni che si ritengono utili nella prospettiva della prossima emanazione del decreto attuativo.

Premessa

Il 25 maggio 2018 è divenuto applicativo anche in Italia il Regolamento (UE) 679/2016[1] ossia il Regolamento generale sulla protezione dei dati (di seguito denominato anche GDPR, acronimo derivante dalla denominazione inglese *General Data Protection Regulation*). L'approssimarsi di tale data ha sollevato crescenti polemiche a causa della complessità delle attività richieste ai destinatari e delle incertezze operative di cui è stato complice – suo malgrado – il legislatore italiano. Alla scadenza del termine – non solo in Italia, ma specialmente nel nostro Paese – molti non si sono presentati in regola con tutte le prescrizioni, rimanendo di conseguenza esposti alle – peraltro elevate – sanzioni da esso previste.

Il GDPR, in effetti, rappresenta l'innovazione più importante degli ultimi anni. Esso non introduce particolari cambiamenti all'impianto complessivo del sistema della protezione dei dati personali, tuttavia presenta due caratteristiche che creano notevoli difficoltà applicative. Anzitutto, le prescrizioni diventano più stringenti per effetto di meccanismi che richiedono la ridefinizione delle procedure interne e la riformulazione dei rapporti con dipendenti, collaboratori, fornitori, clienti o utenti. In secondo luogo, la norma impone ai destinatari di cambiare l'approccio alla gestione dell'informazione, costringendo ad un monitoraggio costante delle misure di sicurezza tecnologiche ed organizzative. Soprattutto questo secondo aspetto – che implica la costruzione di una vera e propria "cultura della sicurezza informatica" – rappresenta lo sforzo più consistente,

[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 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 GUUE L 119 del 4.5.2016, pagg. 1–88.

soprattutto se a tale onere si aggiungono gli inconvenienti della congiuntura economica che stiamo attraversando.

In questa sede ci si propone di introdurre brevemente le novità del GDPR tentando di individuare le esigenze a cui esso intende fare fronte e di compiere alcune valutazioni che tuttavia, visto il ritardo nel recepimento da parte del legislatore italiano, non possono che essere preliminari. Specificamente, nel presente contributo si delinea anzitutto lo stato di sviluppo attuale della "Società dell'Informazione" nel quadro comunitario; in secondo luogo si offre una descrizione sommaria del contesto normativo in cui il GDPR si colloca; in terzo luogo si forniscono alcuni cenni alle più rilevanti novità di tale disciplina; in quarto luogo si accenna ad alcune questioni di particolare delicatezza per il diritto del lavoro; da ultimo si propongono alcune valutazioni finali.

La "Società dell'Informazione" in Unione Europea tra presente e futuro

È noto che la tecnologia costituisce ormai una parte consistente dell'esperienza contemporanea di ciascuno di noi. A tal proposito, l'Unione Europea sottolinea come «[…] *Le tecnologie dell'informazione e della comunicazione (TIC) non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni*»[2]. In termini più specifici, l'informazione, sia in senso comune – come infrastruttura tecnologica – sia in senso tecnico – come insieme di dati – che in senso figurato – come organizzazione di processi sociali – è divenuta un fattore essenziale per il presente e il futuro della nostra società. Questa è la ragione per cui in tutti gli ordinamenti del mondo si assiste ad un notevole sforzo per disciplinare tutto ciò che ne è veicolo o espressione. Nel panorama dell'Unione Europea, alcuni recenti documenti in tema di criptovalute[3], disinformazione[4], intelligenza artificiale[5] manifestano la rilevanza delle questioni sollevate, l'urgenza di risposte di ampio respiro e l'esigenza che esse siano adottate con una visione di lungo termine.

I dati, in generale, possono essere considerati gli atomi della "Società dell'Informazione". I vantaggi derivanti dalla loro analisi e interpretazione hanno un valore che può essere molto elevato. Poiché i dati non esistono in natura – essendo entità artificiali – e non hanno consistenza materiale – a differenza dei tradizionali beni giuridici – si è reso necessaria la creazione di un "ecosistema" normativo nel quale possono trovare soddisfazione gli interessi economici coinvolti nella loro raccolta, elaborazione, utilizzo e condivisione[6]. In questo senso la stessa giuridicità può essere concepita come una sorta di tecnologia, ossia come un artefatto in cui sono descritte le interazioni tra "agenti intenzionali" – categoria che comprende indifferentemente uomini e macchine, ma a ben vedere anche animali – ed i processi generati nel loro ambiente. In massima sintesi, il diritto non è concepito tanto in termini contenutistici – ciò implicherebbe l'imprescindibilità di determinati valori – o in modo imperativistico – mancando un effettivo comando assistito da sanzione – quando come un insieme di "istruzioni" integrato da meccanismi di retroazione che "sterilizzano" il potere in un sistema di controllo impersonale e formalizzato[7].

---

[2] Considerando (1), Proposta di Regolamento UE relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea, COM(2017) 495 final del 13.9.2017.

[3] Proposta di Direttiva che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE, COM/2016/0450 final - 2016/0208 (COD), approvata il 14 maggio 2018.

[4] COM(2018) 236 final, *Tackling online disinformation: a European Approach*, 26.4.2018.

[5] COM(2018) 237 final, *Artificial Intelligence for Europe*, 25.4.2018. Curiosamente il documento ha una data precedente pur avendo un numero progressivo superiore.

[6] La prospettiva per cui la definizione dei rapporti giuridici è preliminare alla creazione di quelli economici descrive fedelmente il fenomeno in questo caso. Per un approfondimento, cfr. NATALINO IRTI, *L'ordine giuridico del mercato*, 6 ed., GLF Editori Laterza, Roma-Bari (Libri del tempo; 349), 2016.

[7] Per apprezzare sotto il profilo teoretico i contenuti della concezione tecnologica della giuridicità, cfr. in Italia UGO PAGALLO, *Il diritto nell'eta dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessita sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli (Digitalica, collana diretta da Ugo Pagallo; 12), 2015. Per comprendere i presupposti di tale visione è utile fare riferimento agli studi che si sono sviluppati negli

Alla luce delle considerazioni appena svolte è più facile comprendere come oggi informatica e diritto tendano a compenetrarsi soprattutto all'interno di organizzazioni complesse. Ciò si può sperimentare empiricamente per il fatto che prescrizioni giuridiche e limitazioni tecnologiche si presentano allo stesso modo: tramite l'interfaccia con cui gli utenti di servizi di vario genere – privati o pubblici – scambiano dati con i loro interlocutori. In termini concettuali, il flusso di informazione in cui siamo immersi è determinato a monte dal *design* che è stato progettato per rendere più efficiente la trasmissione di informazione.

La novità del GDPR è proprio questa: la norma giuridica richiede di incorporare il rispetto del diritto nelle piattaforme tecnologiche e nei processi organizzativi in modo che l'attività produttiva – la fornitura di beni e servizi o di prestazioni professionali – integri le cautele inerenti il trattamento dei dati personali. Forse è la prima volta che ciò accade in modo così evidente, ed è presumibile che sia questa la vera ragione per cui è così difficile per i destinatari adeguarsi ad essa. In massima sintesi, la protezione dei dati personali diventa l'infrastruttura del sistema di controllo informatico-giuridico di tutte le interazioni che ciascuna entità organizzativa – pubblica o privata – ha con il suo "ecosistema" sociale.

Peraltro, in sede applicativa vi è un ulteriore elemento di difficoltà, data dalla "complessità" dell'ordinamento giuridico[8]. Non soltanto i tradizionali "formanti" del diritto[9] – legislazione, giurisprudenza e dottrina – fanno riferimento a diversi ordinamenti – diritto internazionale[10], diritto comunitario, diritto statuale, autonomie locali – ma essi sono anche integrati da espressioni più sofisticate di giuridicità: per esempio, accanto a provvedimenti che decidono casi concreti – analogamente alle comuni sentenze giudiziali – vi sono i pareri, le autorizzazioni generali[11], ma soprattutto le Linee guida[12] e i codici deontologici[13]. Il punto di raccordo tra la formulazione astratta delle disposizioni, l'interpretazione collettivamente elaborata dai giuristi e i casi concreti dell'esperienza giuridica è oggi integrato da molteplici strumenti di "controllo" o di retroazione – non solo tecnologici ma anche organizzativi – che plasmano indirettamente le relazioni sociali in funzione di una maggiore efficienza degli scambi[14].

---

ultimi quindici anni in tema di "Filosofia dell'Informazione". A tal proposito, cfr. LUCIANO FLORIDI, *The philosophy of information*, Oxford-New York, Oxford University Press, 2011; ID, *The 4th Revolution. How the infosphere is reshaping human reality*, tr. it. di Massimo Durante, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina (Scienza e idee; 279), 2017 (2014).

[8] A tal proposito è interessante MARIO G. LOSANO, *Diritto turbolento*, in «Rivista internazionale di filosofia del diritto», LXXXII n. 3 (2005), pp. 403-430.

[9] Per un'introduzione al concetto di "formante del diritto", cfr. RODOLFO SACCO, voce *Formante*, in *Digesto delle discipline privatistiche - Sezione civile*, vol. VIII Esp-Ge, Torino, UTET, 1993, pp. 438-442.

[10] Vale la pena di ricordare che nella sessione del Comitato dei Ministri del Consiglio d'Europa tenutasi ad Elsinore (Danimarca) nei giorni 17 e 18 maggio 2018 è stato approvato il Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE n. 108) stipulata a Strasburgo il 28 gennaio 1981. Il suo scopo è aggiornare la Convenzione e il Protocollo addizionale concernente le autorità di controllo ed i flussi transfrontalieri (STE n. 181) del 2004.

[11] Il Garante per la protezione dei dati personali ai sensi dell'art. 40 D. Lgs. 196/2003 aveva il potere di emanare autorizzazioni di carattere generale e astratto.

[12] Le Linee guida contengono spiegazioni delle disposizioni e indicazioni pratiche corredate da esempi esplicativi. Oltre a quelle emanate dall'Autorità Garante nazionale, è opportuno menzionare quelle del Gruppo di lavoro istituito ai sensi dell'art. 29 della Direttiva 95/46/EC (abbreviato WP29) e riguardanti: il diritto alla portabilità dei dati (WP242 riviste il 27.10.2017), il Responsabile per la protezione dei dati personali (WP243 riviste il 30.10.2017), le autorità di controllo capofila (WP244 riviste il 31.10.2017), la valutazione di impatto (WP248 riviste il 13.10.2017), le sanzioni amministrative (WP253 riviste il 13.2.2018), la notifica di *data breach* (WP250 riviste il 13.2.2018), la profilazione (WP251 riviste il 13.2.2018), la formulazione del consenso (WP259 riviste il 16.4.2018), la trasparenza (WP260 riviste il 13.4.2018). Il WP29 è un organo consultivo dell'Unione Europea composto di rappresentanti delle Autorità per la protezione dei dati personali di ciascuno Stato Membro e del Garante europeo della protezione dei dati. Esso è stato sostituito dal GDPR con il Comitato europeo per la protezione dei dati.

[13] Cfr. art. 12 D. Lgs. 196/2003. La rilevanza delle discipline di settore è ancora maggiore ai sensi del GDPR.

[14] Per un inquadramento della visione adottata in sede comunitaria, cfr. LUCIANO FLORIDI (a cura di), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, Springer International Publishing (Open Access, 2015). Si tratta di un volume pubblicato con il patrocinio dell'Unione Europea.

Il contesto del GDPR: dall'obiettivo del "Mercato Unico Digitale" nell'Unione Europea all'impatto nell'ordinamento interno

Il GDPR rappresenta l'ultima novità di un articolato quadro normativo stratificatosi nel corso degli ultimi anni. Tale panorama di recente è stato sottoposto a svariati interventi di revisione per tre principali motivi: anzitutto nuove tecnologie (per esempio, *social networks*, *cloud computing, blockchain*) hanno reso obsolete le previgenti disposizioni o che comunque ne hanno resa problematica l'applicazione; in secondo luogo, l'incremento del numero di Stati Membri, con l'ulteriore esigenza di imporre regole più ampiamente condivise per la regolamentazione di un mercato più esteso; in terzo luogo, la definizione di una strategia funzionale alla creazione di un "Mercato Unico Digitale"[15] per promuovere la "economia europea dei dati" come fattore determinante nell'incremento del Prodotto Interno Lordo dell'Unione Europea[16].

Dell'evoluzione del diritto in tema di "Società dell'Informazione" si possono fornire alcuni esempi. Per quanto concerne le firme elettroniche, dalla Direttiva 1999/93/CE[17] venne stabilito quasi venti anni fa un quadro normativo con cui si conferiva rilevanza giuridica alle credenziali di autenticazione e di identificazione, stabilendo meccanismi di imputazione dei documenti elettronici. Tale disciplina, che ha consentito di avviare la dematerializzazione delle risorse documentali all'interno di tutti gli Stati Membri, è stata riformata dal Regolamento (UE) 910/2014 c.d. "eIDAS"[18], che ha permesso di far circolare i documenti informatici anche fuori dai singoli ordinamenti, legittimandone il reciproco riconoscimento e contribuendo ad incrementare la circolazione dei beni e dei servizi nella UE. Del resto, la Direttiva 2000/31/CE sul commercio elettronico[19] aveva l'obiettivo di regolare l'allora nascente mercato degli *Internet Service Providers*, stabilendo tutele nei loro confronti – in particolare il principio dell'assenza di obbligo di sorveglianza (art. 17) – ed obblighi informativi verso degli utenti. La recente Direttiva (UE) 2016/1148 c.d. N.I.S (dall'acronimo inglese *Network Information Security*)[20] inserisce tali operatori economici all'interno di una struttura organizzativa predisposta per garantire la sicurezza dell'informazione, attribuendo loro specifici compiti e obblighi di collaborazione con le istituzioni pubbliche nelle ipotesi di incidenti su larga scala come attacchi terroristici o calamità naturali. Si tratta in entrambi i casi di modifiche normative imposte dall'innovazione tecnologica e dalla scoperta di nuove vulnerabilità.

Per quanto concerne in particolare la protezione dei dati personali, è importante sottolineare che il GDPR si propone non solo di sostituire la Direttiva 95/46/CE[21], abrogandola a partire dal 25 maggio 2018 (art.

---

[15] Cfr. COM/2015/192 final, Strategia per il mercato unico digitale in Europa, del 6.5.2015.

[16] COM(2017) 9 final, Costruire un'economia dei dati europea, del 10.1.2017: «*Il valore dell'economia dei dati nell'UE è stato stimato a 257 miliardi di euro nel 2014, pari all'1,85% del PIL dell'UE2, passati a 272 miliardi di euro nel 2015, ossia all'1,87% del PIL dell'UE (per un incremento annuo del 5,6%). La stessa stima prevede che, istituendo per tempo un assetto programmatico e giuridico per l'economia dei dati, il suo valore potrà raggiungere i 643 miliardi di euro nel 2020, pari al 3,17% del PIL complessivo dell'UE*», pag. 2.

[17] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, in GUCE n. L 013 del 19.1.2000 pag. 12–20.

[18] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, in GUUE L 257 del 28.8.2014, pagg. 73–114. Il provvedimento è entrato in vigore il 1° luglio 2016. L'acronimo "eIDAS" deriva dall'inglese *electronic IDentification Authentication and Signature*.

[19] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (c.d. Direttiva sul commercio elettronico), in GUCE L 178 del 17.7.2000, pagg. 1–16.

[20] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, in GUUE L 194 del 19.7.2016, pagg. 1–30. Lo schema di decreto attuativo è stato approvato dal Governo il 16 maggio 2018. Alla data in cui il presente contributo è stato consegnato all'Editore non è stato ancora pubblicato in Gazzetta Ufficiale.

[21] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in GUCE L 281, 23.11.1995, pagg. 31–50.

94 GDPR), ma anche di integrare la Direttiva 2002/58/CE[22] (art. 95 GDPR)[23]. A tal proposito, si tenga conto che, come avvenuto nell'evoluzione della normativa sulle firme elettroniche, si è utilizzato lo strumento del Regolamento invece della Direttiva proprio perché non si ritiene più sufficiente il perseguimento di comuni obiettivi da parte degli Stati Membri, reputando indispensabile vincolare tutti gli operatori ad un regime giuridico omogeneo. Si consideri altresì che il GDPR è solo una delle tre componenti del c.d. "pacchetto privacy": è certamente il provvedimento con gli effetti più immediati e dirompenti, ma insieme ad esso sono state emanate due Direttive che introducono norme concernenti la protezione dei dati personali in settori specifici. Si tratta della Direttiva (UE) 680/2016[24], relativa allo scambio di dati investigativi tra autorità giudiziarie, e della Direttiva (UE) 681/2016[25] che riguarda la condivisione dei codici di prenotazione nei mezzi di trasporto pubblico.

Occorre ammettere che il recepimento del GDPR in Italia è stato più complicato che negli altri Stati membri anche a causa della contingente situazione di stallo istituzionale. È ben vero che il legislatore comunitario, nella consapevolezza della portata innovativa del provvedimento, aveva specificamente previsto di sospenderne l'applicazione nei primi due anni dall'entrata in vigore (art. 99 comma 2 GDPR) anche per dare tempo agli Stati Membri di adeguare le norme interne, tuttavia solo nell'ottobre 2017 – e quindi con un significativo ritardo – il nostro Parlamento conferì delega legislativa al Governo[26]. Quest'ultimo esercitò tale potestà emanando il 21 marzo 2018 – il sabato precedente alle dimissioni, presentate il 24 marzo successivo – uno schema di Decreto Legislativo che – almeno in una delle prime versioni trapelate e subito diffusasi in Rete – suscitò reazioni contrariate tra gli addetti del settore, in particolare per la previsione di totale abrogazione del previgente D. Lgs. 196/2003[27] contenuta nell'art. 101. In effetti qualche perplessità era legittima poiché, la Legge Delega prevede, tra l'altro, di "abrogare espressamente le disposizioni incompatibili" (art. 13 c. 3 lett. a), nonché di modificare le altre "limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili" del GDPR (art.13 c. 3 lett. b).

Come sottolineato dal Garante nel Parere espresso sullo schema di Decreto legislativo emanato in recepimento al GDPR[28], per il futuro della disciplina dei dati personali si prospetta un regime giuridico

---

[22] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in GUCE L 201, 31.7.2002, p. 37–47.

[23] Tra le opere introduttive di respiro comunitario, cfr. PAUL VOIGT E AXEL VON DEM BUSSCHE, *The EU general data protection regulation (GDPR). A practical guide*, Cham, Springer, 2017. Per un'analisi degli istituti con riferimento al diritto interno, cfr. LUCA BOLOGNINI, ENRICO PELINO E CAMILLA BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016; GIUSELLA FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli (Le riforme del diritto italiano; 35), 2017.

[24] 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, in GUUE L 119 del 4.5.2016, pagg. 89–131. Tale normativa è stata recepita con il Decreto Legislativo 18 maggio 2018, n. 51, in GU n.119 del 24.5.2018.

[25] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, in GUUE L 119 del 4.5.2016, pagg. 132–149. Tale normativa è stata recepita con il Decreto Legislativo 21 maggio 2018, n. 53, in GU n.120 del 25.5.2018.

[26] Legge 25 ottobre 2017, n. 163, Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea, c.d. "Legge di delegazione europea 2016-2017", in GU n. 259 del 6.11.2017. La delega è prevista all'art. 13.

[27] Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, in GU n.174 del 29.07.2003, S.O. n. 123.

[28] In data 22 maggio 2018 il Garante sulla Protezione dei Dati Personali ha emesso parere favorevole – condizionato al rispetto delle condizioni poste e all'accoglimento delle osservazioni compiute – (doc. web n. 9163359) sullo schema di Decreto di adeguamento presentato alle Camere il 10 maggio precedente. Anche per effetto di tali valutazioni le Commissioni parlamentari incaricate per l'esame del provvedimento hanno stabilito di iniziare un ciclo di audizioni informali per approfondire le questioni sollevate. Di conseguenza il termine ultimo per l'esercizio del potere delegato da parte del Governo è stato prorogato al 21 agosto 2018.

alquanto composito: anzitutto occorre prendere in considerazione il GDPR che – in virtù del primato del diritto comunitario sul diritto interno – è direttamente applicabile nel nostro ordinamento; in secondo luogo rileva il D. Lgs. 196/2003, o meglio quel che ne rimane dopo l'abrogazione espressa delle norme incompatibili e la modifica delle altre.

Bisogna tenere presente che il GDPR non ha solo un impatto diretto – da ciò l'esigenza di modificare il D. Lgs. 196/2003 – ma ha anche un'influenza indiretta sul diritto interno che – stante il primato del diritto comunitario e in mancanza di un intervento esplicito da parte del legislatore – richiede il coordinamento in via interpretativa. I maggiori problemi nell'applicazione del GDPR si pongono in relazione a questo ultimo aspetto, come si vedrà più avanti a proposito delle questioni emergenti nell'ambito giuslavoristico.

Uno sguardo complessivo alle novità del GDPR

Come anticipato in premessa, il GDPR non stravolge le dinamiche su cui da ormai venti anni si regge il sistema della protezione dei dati personali[29] pur prevedendo significative innovazioni. In questa sede si intende proporre una rapida disamina delle novità introdotte distinguendo due profili quello oggettivo, più strettamente connesso al trattamento dei dati in quanto tale, e quello soggettivo, concernente le figure che vi sono coinvolte.

Per quanto concerne il primo punto, vale la pena specificare ulteriormente quattro aspetti degni di particolare considerazione: anzitutto i presupposti delle disposizioni che rappresentano la reale novità del GDPR rispetto alla previgente disciplina, ossia l'approccio "basato sulla valutazione del rischio"; in secondo luogo, la precisazione dei fondamenti del trattamento, vale a dire la definizione delle ipotesi che integrano la "base giuridica" che lo rende legittimo; in terzo luogo, la definizione di alcuni istituti che riguardano le modalità di trattamento, ed in particolare la positivizzazione dei principi di *privacy by design* e *by default*; da ultimo, la previsione dell'obbligo di notifica in caso di incidenti o accessi abusivi (c.d. *data breach*).

Per quanto riguarda i presupposti ideali del GDPR, occorre sottolineare l'importanza attribuita anche nel GDPR alle questioni che riguardano la sicurezza delle informazioni. L'attenzione su tale tema da parte dell'Unione Europea è sempre più elevata, come dimostrano non soltanto nella già menzionata Direttiva (UE) 1148/2016, ma anche altri documenti più recenti relativi al contrasto a reati informatici, terrorismo e criminalità organizzata, come la Raccomandazione C(2017)6100[30], la Risoluzione 2017/2068(INI)[31] e la dichiarazione congiunta JOIN/2017/450[32]. L'approccio complessivo è improntato alla "resilienza", concetto ripreso dall'ecologia che sostanzialmente indica la caratteristica, propria di un essere vivente o di un ecosistema, di ristabilire l'equilibrio interno – e quindi di sopravvivere – in seguito ad una perturbazione subita dall'ambiente. In termini pratici, "resilienza" significa non soltanto ammettere il fatto che la "sicurezza" in generale non è e non può essere una nozione da prendere in termini assoluti, ma anche e soprattutto riconoscere che le misure di sicurezza sono efficaci non in base ad un apprezzamento effettuato in astratto e una volta per tutte, ma alla luce di una valutazione calata nel concreto contesto in cui i dati sono trattati e di una costante sorveglianza sulla loro effettività[33].

---

[29] Si ricorda che in Italia la normativa originaria fu la Legge n. 675 del 31 dicembre 1996, Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, in GU n. 5 dell'8.1.1997, S.O. n. 3.

[30] Raccomandazione C(2017)6100 final, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala, del 13.9.2017. In essa si prevede il coordinamento tra svariati organismi e istituzioni e si considera come una priorità la sicurezza delle infrastrutture, dei sistemi informatici e dei dati a livello internazionale, comunitario e nazionale.

[31] Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI)).

[32] Comunicazione congiunta JOIN/2017/450 final, Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, del 13.9.2017. Su tale documento, vedasi anche la dichiarazione congiunta all'esito del Consiglio Europeo del 20 novembre 2017.

[33] Proprio perché la nostra vita – privata e lavorativa – dipende sempre più dalle infrastrutture tecnologiche (il lettore provi a immaginare le conseguenze sulla sua quotidianità di un black-out prolungato nella fornitura di energia elettrica o di connessione telematica), le istituzioni europee si preoccupano di individuare modelli e strumenti che consentano di

Non è un caso che la "resilienza" sia prevista (art. 32(1)b GDPR) come specifico requisito delle misure di sicurezza nel trattamento dei dati. Per tale ragione, essenzialmente, sono stati eliminati istituti come la notificazione preventiva al Garante[34] o la verifica c.d. mediante "*prior checking*"[35] del rischio intrinseco a determinati trattamenti, e soprattutto è stata superata la distinzione tra "misure minime di sicurezza" (da adottare per evitare responsabilità penale (art. 169 del D. Lgs. 196/2003) e "misure idonee di sicurezza", da predisporre per non incorrere in responsabilità civile (art. 15 D. Lgs. 106/2003, che rimanda all'art. 2050 Codice Civile). La "valutazione di impatto sul trattamento dei dati" (DPIA dall'inglese *Data Protection Impact Assessment*) di cui all'art. 35 GDPR costituisce essenzialmente un processo di monitoraggio continuativo[36] con il quale il titolare documenta le valutazioni effettuate in merito ai più delicati trattamenti di dati personali e le soluzioni adottate per diminuire i rischi e limitare gli eventuali danni. Proprio sulla base della DPIA, titolare o responsabile, in caso di sinistro, devono dimostrare che le misure predisposte erano comunque "adeguate" al trattamento – non solo "necessarie" e nemmeno "idonee" – e che, di conseguenza, «*l'evento dannoso non gli è in alcun modo imputabile*» (art. 82(3) GDPR)[37]. L'onere della prova, che già era invertito nella previgente normativa, è dunque ulteriormente aggravato dal GDPR.

In merito al fondamento del trattamento, l'approccio complessivo di cui al punto precedente ha una interessante implicazione rispetto alle condizioni di liceità del trattamento o «*base giuridica*». Delle sei ipotesi previste dall'art. 6(1) del GDPR[38] è opportuno soffermarsi sulla sesta, che riguarda il perseguimento di un «*legittimo interesse*» da parte del titolare. In questo caso il trattamento è ammesso – beninteso, a prescindere dal consenso – se ed in quanto non prevalgano «*gli interessi o i diritti e le libertà dell'interessato*», soprattutto se quest'ultimo è minorenne. In altri termini, è il titolare a dover effettuare la delicata valutazione sul "bilanciamento" e quindi a dover motivare le ragioni per cui il proprio vantaggio dovrebbe sulle prerogative dell'interessato. Sotto questo profilo si segnala una ulteriore valutazione che il titolare è tenuto a compiere: quella che riguarda la "compatibilità" tra il fine del trattamento oggetto di consenso da parte dell'interessato e finalità diverse da quelle per le quali essi erano stati raccolti. Per valutare tale "compatibilità" occorre in sintesi tenere conto di: (a) "nesso" tra le la finalità del trattamento originario e di quello ulteriore; (b) contesto in cui i dati sono raccolti; (c) natura dei dati personali; (d) possibili conseguenze dell'ulteriore trattamento; (e) sussistenza di garanzie adeguate, come per esempio la cifratura. Evidentemente si tratta in entrambi i casi di apprezzamenti alquanto delicati e quindi opinabili, fonte di giusta preoccupazione da parte dei titolari del trattamento.

---

limitare le vulnerabilità e, in caso di incidenti, sabotaggi o attacchi, di ristabilire il funzionamento degli impianti, soprattutto quelli di comunicazione, nel più breve tempo possibile.

[34] L'art. 37 del D.Lgs. 196/2003 imponeva al titolare di notificare al Garante il trattamento di specifiche categorie di dati (ad esempio, dati genetici, biometrici, nonché "dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi" (art. 37 c. 1 lett. d).

[35] L'art. 17 del D. Lgs. 196/2003 prevedeva per il trattamento di dati c.d. "semi sensibili" – dati personali di particolare rilevanza pur non ricadendo nelle categorie dei dati sensibili o giudiziari – l'adozione di "misure e accorgimenti" sulla base di una valutazione preliminare relativa ai rischi inerenti al trattamento richiesta dal titolare al Garante.

[36] Come precisato dalle Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 (WP 248).

[37] L'adempimento preliminare rispetto alla DPIA consiste nella redazione di un "Registro dei trattamenti" da parte del titolare e del responsabile (art. 30 GDPR). Si tratta essenzialmente di un elenco, che può essere tenuto anche solo elettronicamente, nel quale tali soggetti descrivono le modalità con cui vengono svolte le attività di trattamento dei dati. in esso vengono indicati per esempio le categorie di dati personali e di interessati, le finalità, le misure di sicurezza organizzative e tecnologiche adottate.

[38] «*a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) 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; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento 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 è un minore*».

Per quanto concerne la modalità del trattamento, la concezione tecnologica della giuridicità di cui si riferiva nei primi paragrafi ha trovato concreta applicazione negli studi che propongono di progettare i dispositivi informatici tenendo conto anzitutto della necessità di rispettare precetti giuridici[39]. Nel campo della protezione dei dati personali questa prospettiva di ricerca, sebbene fosse conosciuta e apprezzata da almeno quindici anni, non è riuscita a trovare un riconoscimento normativo fino al nuovo Regolamento (UE), che ha specificamente previsto (art. 25 GDPR) la protezione dei dati fin dalla progettazione (*privacy by design*)[40] e la protezione per impostazione predefinita (*privacy by default*)[41]. La matrice comune di questi due precetti risiede nel principio di "minimizzazione", secondo cui il trattamento deve riguardare soltanto i dati necessari alle specifiche finalità previste. È molto importante osservare che tale approccio non opera soltanto rispetto agli strumenti informatici, poiché ad esso devono essere improntate anche le procedure organizzative. In altri termini, ogni azienda – indifferentemente pubblica o privata – dovrebbe non soltanto adottare dispositivi tecnologici aggiornati, ma anche sottoporsi a un processo di radicale riorganizzazione interna. Ciò impone un considerevole investimento, in termini di risorse economiche e di tempo, che oggi non molti sono in grado di compiere o sono disposti a intraprendere.

Relativamente all'obbligo di notifica, il GDPR prevede che il titolare, qualora subisca una violazione di dati personali, debba informarne senza ritardo le autorità di controllo (art. 33 GDPR) e l'interessato (art. 34 GDPR). In particolare, entro il termine di 72 ore – molto breve, soprattutto se si considera che un evento può verificarsi in prossimità o durante un periodo festivo – deve essere inviata una notifica contenente i dettagli dell'incidente o dell'attacco informatico nonché le indicazioni relative alle misure adottate per rimediare agli eventuali danni. Per fornire la ragione pratica di tale adempimento – che può richiedere un costo ingente per istituzioni e imprese – è sufficiente richiamare un dato contenuto nella Risoluzione 2017/2068(INI) già menzionata: l'80% delle imprese europee non denunciava gli attacchi informatici subiti[42]. Ciò significa non soltanto che vi è scarsissima cura per la sicurezza delle infrastrutture informatiche, ma anche che non vi è alcun rispetto per i dati personali degli interessati. La norma, in altri termini, vuole evitare che, per effetto dell'incuria dei titolari, gli interessati vengono esposti al rischio di divenire a loro volta vittime di fattispecie criminose – come i "furti di identità" – o di agevolare inconsapevolmente la diffusione delle frodi informatiche. Il GDPR, insomma, richiede a tutti – titolari e responsabili – uno sforzo organizzativo per preservare non solo i diritti degli interessati, ma la sicurezza informatica, concepito come interesse collettivo di primaria importanza.

Dopo l'esame dell'aspetto oggettivo, come si diceva, vale la pena affrontare l'elemento soggettivo. Per maggiore chiarezza espositiva si prevede di procedere in modo analitico anche in questo caso, prendendo in considerazione anzitutto le figure "attive" – titolare e responsabile del trattamento, nonché responsabile per la protezione dei dati (c.d. DPO, dall'inglese *Data Protection Officer*) – per poi riprendere quella dell'interessato e accennare ai suoi c.d. "diritti".

Rispetto alle figure attive, vale la pena premettere che il GDPR non reca particolari novità rispetto al "titolare del trattamento" in quanto tale (art. 24 GDPR), ma innova notevolmente rispetto al contesto in cui esso si colloca. Infatti introduce la fattispecie della "contitolarità" e configura due ulteriori soggetti, quella del "responsabile del trattamento" e quella – del tutto nuova – del "responsabile per la protezione dei dati personali".

La contitolarità (art. 26 GDPR) rappresenta la situazione in cui il trattamento viene effettuato congiuntamente da due titolari. In tale ipotesi la norma prevede che i soggetti si accordino per definire reciproche responsabilità e rispettive funzioni al fine di garantire il rispetto delle prerogative degli interessati.

---

[39] Si tratta di una specificazione dell'approccio definito *value sensitive design*.

[40] In base a questo principio il trattamento dei dati deve essere effettuato tenendo conto anzitutto dei rischi intrinseci, la cui valutazione deve precedere la raccolta delle informazioni.

[41] Alla luce di questo precetto il trattamento dei dati deve riguardare solo i dati necessari, sicché tale deve essere l'impostazione predefinita del consenso che l'interessato è chiamato a prestare.

[42] Il dato è contenuto nelle "Considerazioni generali" n. 6.

Il "responsabile del trattamento" (art. 28 GDPR) è definito come il soggetto che tratta dati "per conto" del titolare: tale figura non deve essere confusa con quella avente la medesima denominazione prevista dal previgente regime, né può essere ridotta a mero referente esterno al titolare per il trattamento dei dati di quest'ultimo. Infatti il GDPR costruisce il rapporto tra titolare e responsabile come un incarico che prevede degli obblighi reciproci: essenzialmente il primo deve fornire delle istruzioni documentate al secondo (art. 28(2)a GDPR), il quale deve dimostrare di adottarle. Per tale motivo si può sostenere che la relazione tra titolare e responsabile è il punto in cui si realizza in modo più compiuto un altro dei pilastri del GDPR, ossia il principio di "responsabilizzazione": tutti i soggetti destinatari delle disposizioni del GDPR non devono soltanto adeguarsi ad esso, ma porsi nelle condizioni di poter dimostrare di averlo fatto, qualora venga richiesto in particolare dalle autorità di controllo.

Il "responsabile per la protezione dei dati personali", come si diceva, è la vera novità nella dinamica delle relazioni tra i soggetti del GDPR. Si tratta di una figura con elevate competenze nella materia[43] che deve essere designata da titolare o responsabile quando il trattamento presenta profili di particolare delicatezza (art. 37 GDPR)[44]. È molto importante sottolineare che il DPO non è un semplice consulente esterno, ma un soggetto a cui sono attribuiti molteplici compiti (art. 39 GDPR): accanto a informazione e consulenza a beneficio di interessato e titolare, vi sono infatti la loro sorveglianza e la cooperazione con il Garante nell'accertamento di eventuali illeciti. In massima sintesi, il DPO è una sorta di commissario – il termine inglese *officer* rende l'idea meglio del corrispondente italiano "Responsabile" – che deve operare in modo "proattivo" anche in contrapposizione, se necessario, con gli stessi soggetti che lo hanno nominato. Da tale ultimo rilievo si può facilmente comprendere come la sua posizione sia particolarmente delicata e perché si preveda esplicitamente di evitare situazioni di conflitti di interesse (art. 38(6) GDPR).

Relativamente all'aspetto "passivo", le innovazioni contenute nel GDPR sono state presentate al pubblico come un rafforzamento nella protezione dei dati personali dell'interessato. Ciò è indubbiamente vero non solo in generale, poiché l'intero sistema è concepito per incrementare il livello di sicurezza nella gestione dell'informazione – come illustrato nei precedenti paragrafi – ma anche alla luce delle specifiche disposizioni che, per un verso, incrementano il livello di trasparenza del trattamento e che, per altro verso, rendono più efficaci gli istituti già a disposizione dell'interessato per far valere i propri diritti. Per quanto riguarda il primo aspetto, all'inizio del trattamento è prevista una informativa più specifica, differenziata a seconda che i dati vengano raccolti presso l'interessato (art. 13 GDPR) o meno (art. 14 GDPR). Per quanto concerne il secondo profilo, sono state estese le informazioni che il titolare deve fornire qualora l'interessato eserciti il c.d. "diritto di accesso" (art. 15 GDPR) – a comprendere anche la modalità del trattamento e il periodo di conservazione – ed è stato positivizzato il c.d. "diritto all'oblio" (art. 17 GDPR)[45] che era apparso nell'ordinamento comunitario già nel 2014 per effetto della sentenza "Google Spain" della CGUE[46].

[43] La figura del DPO è descritta nello standard tecnico di recente approvazione UNI 11697:2017: Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza.

[44] In massima sintesi, si richiede il DPO quando: (a) il titolare è una pubblica amministrazione; (b) il titolare tratta dati mediante "monitoraggio regolare e sistematico degli interessati su larga scala"; (c) il titolare tratta su larga scala dati di carattere "sensibile" – cioè "categorie particolari di dati" (art. 9 GDPR) e dati giudiziari (art. 10 GDPR).

[45] Il "diritto all'oblio" può essere considerato come espressione del principio di "minimizzazione" nel trattamento dei dati, poiché opera nei casi in cui il trattamento non è più necessario, il consenso è stato revocato o il trattamento era illegittimo sin dall'origine. Per vero vi è anche un diritto alla limitazione (art. 18 GDPR) che consente all'interessato di graduare le modalità con cui i suoi dati sono trattati richiedendo che essi siano soltanto conservati dal titolare in via provvisoria. Per effetto di tale richiesta ogni altro trattamento è illecito. Vale la pena ricordare anche il "diritto alla portabilità" (art. 20 GDPR) che consiste in una maggiore facilità di trasferimento dei dati tra titolari.

[46] Grand Chamber 13 Maggio 2014, *Google Spain SL, Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317.

Se il rispetto delle prescrizioni del GDPR è assistito da un sistema punitivo molto severo, è vero anche che le sanzioni sono più gravi nelle ipotesi di violazione dei diritti dell'interessato[47]. Ciò è indicativo dell'importanza concretamente attribuita al rispetto di principi come il consenso o la finalità del trattamento.

GDPR, dati personali e diritto del lavoro: l'esempio dei "controlli" del datore di lavoro

In precedenza si era fatto riferimento all'influenza indiretta del GDPR in settori dell'ordinamento nei quali il trattamento dei dati personali non è propriamente oggetto di disciplina bensì l'effetto delle dinamiche relazionali tra i soggetti coinvolti. In ciò il diritto del lavoro ha una posizione privilegiata perché in un contesto aziendale – pubblico o privato – vi sono diversi interessi che devono necessariamente trovare il modo di coesistere nel medesimo ambito. Semplificando si può sostenere che dal lato del datore di lavoro tende a prevalere una logica improntata alla "verticalità" organizzativa del "controllo" dei flussi informativi, mentre da quello del dipendente sembra preponderante una "orizzontalità" collaborativa proiettata verso la "condivisione" delle risorse. Questa contrapposizione peraltro tende a sfumare con la sempre maggiore diffusione di forme di lavoro "agili" o *smart*, rese possibili proprio dall'utilizzo di piattaforme informatiche che, peraltro, talvolta sono gestite da soggetti terzi[48]. Il "controllo" dell'informazione, in altri termini, diventa una componente essenziale del rapporto lavorativo, e ciò a prescindere dalla sua qualificazione giuridica.

Volendo concentrare l'attenzione sull'influenza del GDPR nei rapporti tra datore di lavoro e dipendente, sembra utile distinguere due piani di considerazione: uno più generale e uno più specifico.

In via generale la normativa dovrà essere rivista alla luce delle modifiche apportate dal GDPR dall'istituto del "consenso dell'interessato"[49]. Se da un lato la nuova formulazione tende a superare limiti di tipo formale rispetto a quanto previsto nella normativa previgente, dall'altro vi è un maggiore rigore sotto il profilo sostanziale, sicché se il consenso non è effettivamente spontaneo e specifico, non può essere utilizzato come "base giuridica" e dunque il titolare deve giustificare il trattamento dei dati in altro modo. Le recenti *Linee guida* del Gruppo di lavoro ex art. 29 prendono specificamente in considerazione la situazione di *embalance of power* (n.t. "squilibrio di potere") che si verifica tra il datore di lavoro e il dipendente, osservando come in tale contesto difficilmente si possa configurare un vero e proprio consenso per effetto delle conseguenze negative che l'interessato si può rappresentare nell'eventualità che egli si rifiuti di prestarlo[50]. Secondo il WP29, in sintesi, la validità del consenso ai fini del trattamento dei dati personali in ambito lavorativo deve considerarsi del tutto eccezionale e deve essere dimostrata dal titolare: un compito non impossibile, ma certamente arduo[51]. Di conseguenza, rispetto al trattamento dei dati dei dipendenti occorre prendere in considerazione soprattutto le altre "basi giuridiche" previste dagli artt. 6 e 9 GDPR: prescindendo dalle ipotesi che riguardano gli ordinari adempimenti burocratici che onerano il rapporto lavorativo e le situazioni straordinarie in cui si presenta la necessità di tutelare interessi vitali, sembra inevitabile fare riferimento all'ipotesi del «*legittimo interesse del titolare*», e dunque al problematico bilanciamento con «*gli*

---

[47] Si prevede che le sanzioni amministrative pecuniarie siano "effettive, proporzionate, dissuasive" (art. 83(1) GDPR) graduate secondo una serie molto variegata di criteri (art. 83(2) GDPR) e divise in due grandi categorie a seconda della gravità delle violazioni. L'articolo 83 distingue essenzialmente due categorie di sanzioni, una fino a 10 milioni di euro o, per le imprese, 2% del fatturato mondiale annuo, se superiore (art. 83(4) GDPR); l'altra di importi raddoppiati (art. 83(5) GDPR).

[48] Per un inquadramento teoretico si tenga presente DOMENICO GAROFALO, *Lavoro, impresa e trasformazioni organizzative*, Frammentazione organizzativa e lavoro: rapporti individuali e collettivi, Aidlass, 2017.

[49] «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*» (art. 4(1)11 GDPR).

[50] Linee guida sul consenso WP259 rev. 01, pag. 7.

[51] Bisogna precisare che il consenso non è richiesto per "dati sensibili" (art. 9(2)b GDPR), qualora il trattamento sia necessario per adempiere a obblighi in tema di diritto del lavoro, sicurezza del lavoro e protezione sociale, se ciò è previsto dalla legge o da un contratto collettivo, e sempre che vi siano garanzie appropriate per l'interessato. In altri termini, la previsione di un obbligo normativo giustifica il trattamento dei dati, tuttavia non esclude l'obbligo di adottare misure di sicurezza conformi ai rischi inerenti a tale attività.

interessi o i diritti e le libertà fondamentali dell'interessato» (art. 6(1)f GDPR) utilizzando i criteri sopra indicati.

Con specifico riferimento agli interessi del datore di lavoro, vale la pena osservare che il Regolamento (UE) 679/2016 contiene alcune previsioni che tuttavia mancano di contenuto precettivo. Infatti, all'art. 88(1) GDPR si prevede che gli Stati possano intervenire – tramite legge o contratti collettivi – prevedendo «*norme più specifiche*» per disciplinare determinati aspetti del rapporto lavorativo[52]. Il tenore letterale suggerisce che si ammettono interventi integrativi senza però concedere particolari margini di manovra, di conseguenza bisogna concludere che la normativa vigente debba essere riconsiderata – e rimodellata – in via interpretativa alla luce del GDPR[53]. La disposizione prosegue imponendo peraltro «*misure appropriate e specifiche*» a protezione «*della dignità umana, degli interessi legittimi e dei diritti fondamentali*»[54] in alcune ipotesi particolarmente delicate di trattamento di dati personali, tra le quali è prevista la sorveglianza dei dipendenti. A tal proposito, vale la pena di soffermarsi a considerarne brevemente l'attuale disciplina e valutare l'influenza del GDPR[55].

È noto che la norma di riferimento è l'art. 4 dello Statuto dei Lavoratori[56] così come riformulato per effetto del *Jobs Act*[57]. La disciplina condiziona l'installazione di «*impianti audiovisivi e […] altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*» alla sussistenza di un accordo sindacale, e alla ricorrenza di una tra tre finalità specificamente individuate: «*per esigenze*

---

[52] «[…] *in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di 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 e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro*».

[53] Cfr. in particolare Opinion 2/2017 WP29 *on data processing at work* (8 giugno 2017). In esso si distinguono diversi profili di rischio nel trattamento dei dati personali in ambito lavorativo: processo di selezione del personale, monitoraggio dei dipendenti, sorveglianza tecnologica all'interno del posto di lavoro, controllo tecnologico fuori dal contesto lavorativo, controllo relativo agli orari lavorativi, videosorveglianza, controllo remoto dei veicoli, condivisione dei dati dei dipendenti con soggetti terzi e infine trasferimento all'estero o condivisione con organizzazioni internazionali. Tale classificazione si può rivelare molto utile dal punto di vista operativo nell'attività di valutazione dei rischi concernenti la protezione dei dati personali. Rispetto al previgente regime giuridico, cfr. Opinion 8/2001 WP29 *on the processing of personal data in the employment context* (13 settembre 2001), Working document WP29 *on the surveillance of electronic communications in the workplace* (29 maggio 2002). Sul punto cfr. per quanto riguarda il Consiglio d'Europa, la Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale (Adottata dal Comitato dei Ministri il 1 aprile 2015, nel corso della 1224ma seduta dei rappresentanti dei Ministri).

[54] Il riferimento, come si diceva nel paragrafo precedente, è alle regole "più specifiche" che gli Stati Membri sono autorizzati a stabilire: «*Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro*» (art. 88(2) GDPR).

[55] Si tenga presente che il quadro è alquanto complesso e peraltro non privo di rilevanza internazionale, come confermato da alcune recenti pronunce della Corte Europea dei Diritti dell'Uomo: sentenza (Grand Chamber), 5 settembre 2017, n. 61496/08, *Bărbulescu v. Romania*, commentata in MAURIZIO DALLA CASA, *Controlli su strumenti informatici dopo la sentenza Barbulescu del 2017 della CEDU*, in «Il lavoro nella giurisprudenza», n. 5 (2018), pp. 437-445, nonché sentenza (III sezione), 9 gennaio 2018, *López Ribalda and others v. Spain*, nn. 1874/13 e 8567/13, commentata in ANDREA SITZIA, *Videosorveglianza occulta, privacy e diritto di proprietà. La Corte EDU torna sul criterio di bilanciamento*, in «ADL», n. 2 (2018), pp. 506-522.

[56] 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, in GU 27 maggio 1970, n. 131, c.d. Statuto dei lavoratori.

[57] Per la precisione, la disposizione in discorso è stata oggetto di due interventi. Il primo riguardava la sostituzione da parte del 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, in GU 23 settembre 2015, n. 221, S.O. n. 53. Il secondo invece operò la modifica del comma 1 da parte del Decreto Legislativo 24 settembre 2016 n. 185, Disposizioni integrative e correttive dei decreti legislativi 15 giugno 2015, n. 81 e 14 settembre 2015, nn. 148, 149, 150 e 151, a norma dell'articolo 1, comma 13, della legge 10 dicembre 2014, n. 183, in GU 7 ottobre 2016, n. 235.

organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale» (art. 4 St. Lav. comma 1). Si esclude il ricorso a tale procedura in relazione a «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa»* nonché *«strumenti di registrazione degli accessi e delle presenze*» (art. 4 St. Lav. comma 2). L'utilizzabilità dei dati raccolti «*a tutti i fini connessi al rapporto di lavoro*» è peraltro subordinata alla sussistenza di «*adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*» e al «*rispetto di quanto disposto*» dal D. Lgs. 196/2003 (art. 4 St. Lav. comma 3)[58].

Giurisprudenza e dottrina si sono sforzati di trovare un difficile equilibrio tra l'interesse del datore di lavoro alla tutela del patrimonio aziendale, specialmente mediate i "controlli difensivi"[59] e il diritto alla riservatezza dei dipendenti individuando criteri di valutazione[60] che il Garante per la Protezione dei Dati Personali ha integrato con indicazioni pratiche[61]. Accanto alla regola generale del divieto dei "controlli a distanza" sulla prestazione lavorativa si è ritenuto essenzialmente che la tutela del dipendente non è data dal consenso di quest'ultimo – sulla cui "genuinità" è lecito dubitare – quanto da oggettivi requisiti di necessità, proporzionalità e trasparenza. È evidente che il rispetto di tali condizioni deve essere argomentata con molta attenzione poiché deve essere riferita al caso concreto e richiede la considerazione congiunta di elementi tecnici, organizzativi e giuridici.

Il GDPR non introduce particolari novità sul punto, ma richiede una rigorosa formalizzazione del modo in cui il trattamento viene effettuato, quindi uno sforzo ulteriore sotto il profilo della prova della sussistenza dei requisiti che legittimano il controllo dei dipendenti. Ciò avviene per esempio attraverso lo strumento del "registro dei trattamenti" che ai sensi dell'art. 30 GDPR il titolare e il responsabile sono tenuti a compilare ed esibire all'Autorità di controllo su sua richiesta. Bisogna precisare che la normativa esclude esplicitamente tale obbligo per le aziende con meno di 250 dipendenti «*a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10*». Se, in mancanza di disposizioni specifiche sul punto da parte del legislatore, non si può sostenere che il registro dei trattamenti sia un adempimento esplicitamente richiesto dalla norma al datore di lavoro, sembra tuttavia che esso rappresenti un onere quantomeno utile ed opportuno ai sensi della normativa giuslavoristica per dimostrare il rispetto dei requisiti di legittimità dei controlli sui dipendenti.

Valutazioni finali

L'evoluzione della normativa europea in tema di "Società dell'Informazione" non si conclude con il GDPR. Infatti sono in preparazione ulteriori norme che avranno un consistente impatto nel nostro ordinamento: la proposta di Regolamento (UE) c.d. e-Privacy[62] e la proposta di Regolamento (UE) sui dati non personali[63].

---

[58] Il riferimento all'utilizzabilità dei dati raccolti richiama l'art. 11 comma 2 del D. Lgs. 196/2003.

[59] Come è noto, la giurisprudenza include in tale specifica categoria la sorveglianza che ha per oggetto la tutela del patrimonio aziendale, non «*l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro*» come stabilito in una decisione che costituisce un autorevole precedente, Cassazione civile, sez. lav., 17/07/2007, n. 15892 in "Riv. it. dir. lav." (2008), 3, II, pag. 714 con nota di Vallauri.

[60] Di recente sull'utilizzabilità delle registrazioni da videosorveglianza in sede penale nei confronti dei dipendenti infedeli, cfr. Cassazione penale, sez. II, 30/11/2017, (ud. 30/11/2017, dep.30/01/2018), n. 4367. Sull'argomento specifico dei controlli informatici cfr. ALBERTO LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli (Studi di diritto del Lavoro, collana diretta da Luisa Galantino e Salvatore Hernandez; 31), 2014.

[61] Linee guida del Garante per la Protezione dei Dati Personali, *Lavoro: le linee guida del Garante per posta elettronica e internet*, in GU n. 58 del 10 marzo 2007 [doc. web n. 1387522].

[62] COM (2017) 10 final del 10.1.2017, Proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), Procedimento 2017/3(COD).

[63] COM(2017) 495 final del 13.9.2017, Proposta di Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, Procedimento 2017/0228(COD).

In sintesi, l'Unione Europea si sta proiettando con slancio verso l'economia digitale e ciò impone agli Stati Membri di seguirla in questa sfida.

L'Italia, anche per contingenti vicende istituzionali, si è trovata impreparata alla scadenza del GDPR, tuttavia, se è vero che il nostro legislatore avrebbe potuto fare di meglio, è vero anche che istituzioni e imprese italiane avrebbero potuto fare di più. Purtroppo non è la prima volta che viene persa un'occasione preziosa per valorizzare le nostre risorse informatiche: basta ricordare quanto verificatosi all'avvento del D. Lgs. 196/2003, quando le prescrizioni relative ad alcuni adempimenti giudicati eccessivamente onerosi – in particolare la redazione del "documento programmatico per la sicurezza" (art. 34 c. 1 lett. g) D. Lgs. 196/2003) – vennero sospese in via di prima applicazione e poi definitivamente abrogate su pressione delle categorie sociali[64]. Il fatto che il GDPR sia di provenienza comunitaria ha impedito che questa volta si giungesse ad un epilogo analogo ma non ha evitato un comune disinteresse.

L'esempio dei controlli difensivi è interessante anche perché rivela un aspetto paradossale. Infatti, se è vero che ai sensi dell'art. 4 comma 3 L. 300/1970 il rispetto delle prescrizioni in tema di dati personali è previsto come condizione della loro utilizzabilità anche a fini disciplinari, è vero anche che il mancato adeguamento al GDPR rischia di ritorcersi contro il titolare non solo per l'esposizione alle sanzioni amministrative pecuniarie *ivi* previste, ma anche perché lascia adito alla possibilità di eccepire la legittimità delle sanzioni comminate ai dipendenti[65]. Il pericolo è che il datore di lavoro inadempiente ai sensi del GDPR – e qui descriviamo una situazione alquanto diffusa – si possa ritrovare a decidere se punire il dipendente infedele oppure lasciar correre per non esporsi alle sanzioni previste per la violazione dei dati personali.

Alcune volte le congiunture istituzionali favoriscono i processi di rinnovamento dei sistemi giuridici, altre volte li ostacolano. Nel caso del GDPR a ciò si è accompagnata un'evoluzione che ha portato una diffusa inerzia a trasformarsi progressivamente in frenesia che si è espressa a tratti in scomposte reazioni o nell'abbandono ad un rassegnato sconforto. È verosimile – ma ovviamente nessuno lo garantisce – che i prossimi mesi saranno dedicati ad una fase di progressivo assestamento durante la quale sarà possibile familiarizzare con istituti giuridici e dinamiche nuove. Sarebbe peraltro auspicabile che il legislatore, quando la contingente instabilità sarà superata, possa intervenire in modo organico sul diritto interno per coordinare un insieme di aggiustamenti utili a risolvere problemi come quello esemplificato.

Bibliografia

BOLOGNINI, LUCA, ENRICO PELINO E CAMILLA BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016

DALLA CASA, MAURIZIO, *Controlli su strumenti informatici dopo la sentenza Barbulescu del 2017 della CEDU*, in «Il lavoro nella giurisprudenza», n. 5 (2018), pp. 437-445

FINOCCHIARO, GIUSELLA (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli (Le riforme del diritto italiano; 35), 2017

[64] Più precisamente, il periodo di sospensione previsto dall'art. 180 D. Lgs. 196/2003 fu prorogato ben quattro volte. Successivamente venne ridotto l'ambito di applicazione di tale misura disponendo la sostituzione del Documento Programmatico per la Sicurezza con un'autocertificazione (art. 29, c. 1, Decreto Legge 25 giugno 2008, n. 112 in G.U. 25 giugno 2008, n. 147, S.O. n. 152). Tale adempimento venne infine abrogato dall'art. 45 del Decreto Legge 9 febbraio 2012, n. 5 in G.U. 9 febbraio 2012, n. 33, S.O. n. 26.

[65] L'inutilizzabilità dei dati acquisiti in violazione della relativa disciplina è specificamente prevista dall'art. 2 novies dello schema di Decreto Legislativo presentato alle Camere.

FLORIDI, LUCIANO, *The philosophy of information*, Oxford-New York, Oxford University Press, 2011

---, *The 4th Revolution. How the infosphere is reshaping human reality*, tr. it. di Massimo Durante, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina (Scienza e idee; 279), 2017 (2014)

--- (a cura di), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, Springer International Publishing (Open Access, 2015

GAROFALO, DOMENICO, *Lavoro, impresa e trasformazioni organizzative*, Frammentazione organizzativa e lavoro: rapporti individuali e collettivi, Aidlass, 2017,

IRTI, NATALINO, *L'ordine giuridico del mercato*, 6 ed., GLF Editori Laterza, Roma-Bari (Libri del tempo; 349), 2016

LEVI, ALBERTO, *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli (Studi di diritto del Lavoro, collana diretta da Luisa Galantino e Salvatore Hernandez; 31), 2014

LOSANO, MARIO G., *Diritto turbolento*, in «Rivista internazionale di filosofia del diritto», LXXXII n. 3 (2005), pp. 403-430

PAGALLO, UGO, *Il diritto nell'eta dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessita sociale, lotta per il potere e tutela dei diritti*, Torino, Giappichelli (Digitalica, collana diretta da Ugo Pagallo; 12), 2015

SACCO, RODOLFO, voce *Formante*, in *Digesto delle discipline privatistiche - Sezione civile*, vol. VIII Esp-Ge, Torino, UTET, 1993, pp. 438-442

SITZIA, ANDREA, *Videosorveglianza occulta, privacy e diritto di proprietà. La Corte EDU torna sul criterio di bilanciamento*, in «ADL», n. 2 (2018), pp. 506-522

VOIGT, PAUL E AXEL VON DEM BUSSCHE, *The EU general data protection regulation (GDPR). A practical guide*, Cham, Springer, 2017