

INTRODUZIONE

Negli ultimi decenni abbiamo assistito ad un rapido sviluppo delle tecnologie informatiche che, inizialmente rappresentate da semplici elaboratori elettronici per calcoli che un tempo erano considerati complessi, si sono trasformate in *portable devices* che ineriscono ad ogni ambito della vita quotidiana dell'individuo ponendolo in costante connessione, attraverso le infrastrutture del *web*, a miliardi di suoi simili. In questo contesto sono aumentate esponenzialmente le relazioni umane grazie alle nuove possibilità offerte dal mondo digitale, dai semplici mezzi di comunicazione elettronici che permettono a persone distanti fra loro nell'ordine di migliaia di chilometri di poter comunicare istantaneamente attraverso piattaforme gestite da privati (i c. d. *social*), alle nuove occasioni di contatto tra consumatore e venditore createsi nell'ambito di sistemi di *e-commerce* che esorbitano dai tradizionali limiti territoriali e culturali a cui il mercato, storicamente, ci aveva abituati.

Il fenomeno si è ulteriormente strutturato in modalità ancora incerte a causa dei recentissimi progressi dell'*AI* e degli algoritmi di automatizzazione, macchine in grado di apprendere autonomamente attraverso sistemi di *deep learning* che partendo da istruzioni impartite durante la loro progettazione possono raggiungere risultati non sempre prevedibili dal creatore. L'automazione gioca un ruolo fondamentale nelle c. d. attività di profilazione che utilizzano la gigantesca massa di dati (da qui, il termine *Big Data*) fornita dagli utenti *online* sulle loro caratteristiche personali, abitudini di vita e preferenze per prendere decisioni che li riguardano e dirigerli verso ciò che la macchina crede sia la scelta più adatta a loro.

L'idea di una società ormai basata su decisioni automatizzate che ineriscono ad ogni aspetto della vita personale, dallo *shopping* ai rapporti di lavoro, dalla sicurezza urbana alla fruizione di servizi pubblici, compresi i trattamenti sanitari, è ormai comunemente accettata. O forse sarebbe più corretto dire "ignorata", se pensiamo che fino a qualche decennio fa consideravamo gli scritti di *Isaac Asimov*, su robot che prendono decisioni per gli esseri umani, la rappresentazione immaginaria di uno spaventoso futuro distopico, e la paura di un *Big Brother* di ispirazione *Orwelliana* che controlla ogni nostro movimento, parola o pensiero

sembrava definitivamente cessata con la fine dei totalitarismi. Eppure mai come oggi è stato così forte il timore di dirigerci verso quel tipo di società, dei cui rischi manca ai più una consapevolezza, a causa anche dell'opacità che caratterizza le tecnologie di automazione, tanto da esser stato coniato il termine *black box society* per riferirsi all'attuale modello di comunità.

È in questo contesto che assume un'importanza assai rilevante la protezione dei dati personali, la tutela della *privacy*, principio poco valorizzato dagli Stati moderni all'inizio della loro storia o relegato all'ambito della stampa e della riservatezza delle persone più celebri. L'Italia è arrivata in ritardo anche rispetto agli altri ordinamenti europei nel processo di riconoscimento dei nuovi diritti della personalità, tanto d'aver introdotto la prima normativa sulla *privacy* solo nel 1996.

Dall'altro lato, sul fronte comunitario, l'Unione Europea ha avviato un lungo percorso di legiferazione negli ultimi 30 anni, integrato dalla propria giurisprudenza e da quella degli Stati membri, e dalla grande quantità di *soft law* in materia affidata ai propri organi e a comitati stabiliti *ad hoc* – il Gruppo art. 29, costituito dalle autorità nazionali di controllo del settore, è un esempio. Tale percorso non può dirsi certamente finito data la moltitudine di progetti di riforma e di innovazione che il legislatore porta avanti per rispondere all'esigenza, da un lato, di inseguire una società in rapidissima evoluzione nella quale sorgono nuove criticità e rischi per la *privacy* e allo stesso tempo, come vedremo, di anticipare i mutamenti che avverranno e prevedere una disciplina abbastanza flessibile da non lasciare mai vuoti normativi.

In questo elaborato, dopo aver affrontato un riepilogo dei passi fondamentali che hanno portato al riconoscimento del diritto alla riservatezza, l'analisi comincerà proprio dal Regolamento Generale sulla Protezione dei Dati, che rappresenta il fulcro della disciplina in materia.

Partendo dalla sua genesi e dagli atti che lo hanno preceduto, saranno esposti i principi generali e le garanzie previste per il c.d. trattamento dei dati personali e descritti i soggetti a cui le norme si rivolgono. Ci si soffermerà in particolare sulla tutela del minore, soggetto debole a cui i legislatori europeo e nazionali hanno dedicato un'attenzione particolare.

Il secondo capitolo sarà dedicato in maniera specifica ai trattamenti automatizzati e alla profilazione, sopraccennati, dei quali si spiegheranno i presupposti giuridici e le garanzie previste dalla normativa in relazione ai principali pericoli che in essi sono da più parti riconosciuti. Una sezione sarà dettagliatamente rivolta all'analisi delle responsabilità, dei mezzi di tutela e dei profili sanzionatori previsti in ambito europeo e trasposti (e talvolta ampliati) anche nel nostro ordinamento, individuando alcuni specifici casi giudiziari noti.

Infine, l'ultimo capitolo si soffermerà sull'attuale uso delle tecniche di trattamento automatizzato dei dati e di profilazione in relazione ai numerosi ambiti della società in cui essi, come accennato, sono coinvolti da diversi anni. Questa ricerca è stata improntata ad una prospettiva che tiene conto delle diverse opinioni che di volta in volta sono state avanzate verso queste tecnologie, alcune favorevoli ad una loro maggiore integrazione, altre invece più caute e tese ad una regolamentazione più restrittiva. Essendo un ambito giuridico ancora in fase di definizione, parte dello scritto è dedicato anche ai vari progetti di implementazione di queste tecnologie, soprattutto in relazione alla c. d. giustizia predittiva. Durante il lavoro è stato svolto un confronto costante tra la disciplina di matrice europea e quella specifica dell'ordinamento italiano (in particolare, il D.Lgs. n. 196/2003 e il D. Lgs. n. 101/2018 di adeguamento al Regolamento) e, allo stesso tempo, tra la normativa UE e quella di altre realtà nazionali al di fuori dell'Europa. Il paragrafo finale approfondirà nel dettaglio l'intelligenza artificiale e la recente regolamentazione comunitaria del settore, unica al mondo, focalizzandosi su alcuni primi interventi portati avanti dalle autorità nazionali della privacy.

Lo scopo del testo è quello di presentare sinteticamente, per quanto possibile, un settore del diritto in costante evoluzione, sul quale è aperto un ampio dibattito dottrinale, riportato più volte nell'elaborato, che trascende i limiti nazionali e accomuna giuristi provenienti da più parti del mondo. Una materia che, forse, non riceve ancora l'attenzione che meriterebbe nelle aule universitarie e, a volte, nemmeno dagli stessi operatori del diritto italiano.

CAPITOLO 1. GDPR. TRATTAMENTO DEI DATI PERSONALI. CONSENSO

1.1 Regolamento Generale sulla Protezione dei Dati

«Ogni individuo ha diritto alla vita, alla libertà e alla sicurezza della persona»¹, con queste parole l'art. 3 della Dichiarazione Universale dei Diritti Umani dell'ONU sancisce un principio fondamentale per la storia della civiltà umana del dopoguerra. La società necessita di regole per dare un ordine al caos a cui gli individui sarebbero assoggettati se non esistesse un freno alla libertà di scelta del singolo – è quest'ultimo il principio con cui deve scontrarsi il tessuto normativo. Globalizzazione e progresso tecnologico caratterizzano la modernità in cui viviamo ed è in questo contesto che siamo consapevoli dell'importanza che riveste il diritto alla protezione dei dati personali, le cui radici sono ben più in là nel passato rispetto alla nascita di Internet.

Il «diritto a essere lasciati soli» (*the right to be let alone*) fu teorizzato nel 1890 sulla *Harvard Law Review*, in un articolo a firma di *Warren e Brandeis*, relativamente all'uso generalizzato della stampa², strumento certamente in grado di mettere a repentaglio la *privacy* (così oggi definita) dei cittadini³. In Italia il problema della riservatezza sorse in seguito al secondo conflitto mondiale in relazione alla pubblicazione di fatti personali, tramite stampa o prodotti cinematografici, riguardanti la vita di persone celebri in quel tempo.

In un primo orientamento, la Cassazione negò a metà degli anni '50 l'esistenza di un diritto alla riservatezza⁴ sostenendo che non fosse vietato «comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti». La sentenza da cui è tratta la massima aveva ad oggetto la controversia su una pellicola

¹ Assemblea generale delle Nazioni Unite, Parigi, 10 dicembre 1948, *Dichiarazione Universale dei Diritti Umani*, art. 3.

² BRANDEIS L., WARREN II S. D., *The Right to Privacy*, in *Harvard Law Review*, vol. IV, n. 5, 1890, in cui gli autori conclusero con «*it would doubtless be desirable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required*».

³ PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Giuffrè Francis Lefebvre, Milano, 2019, p. 6 ss.

⁴ Cass. 22 dicembre 1956, n. 4487, *Soc. produzione associata Tirrena Asso film c. Caruso*, in *Il Foro Italiano*, Vol. 80, 1957, p. 3-12.

riguardante la vita del tenore *Enrico Caruso* il cui contenuto era ritenuto lesivo della riservatezza e dell'onore dell'artista da parte dei familiari.

Una sola decina d'anni dopo si assiste ad un lieve cambio di indirizzo nella giurisprudenza della Suprema Corte che afferma essere lesiva del diritto assoluto di personalità la «divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito ed ove non sussista [...] un interesse pubblico di conoscenza» ma continuando a ritenere che «non sia ammissibile il diritto tipico alla riservatezza»⁵ – anche qui, la controversia sorge in relazione alla pubblicazione di un'opera (letteraria) riguardante l'amante del duce, *Claretta Petacci*, e alla sua presunta lesività alla reputazione della donna.

Solo nel 1975 la Cassazione muta definitivamente orientamento e afferma che «il nostro ordinamento riconosce il diritto alla riservatezza», ancorandolo alle norme civilistiche che tutelano la vita familiare e personale e, ovviamente, all'art. 2 della Costituzione sui diritti inviolabili della persona. Nella stessa sentenza – anche in questo caso sorta nell'ambito di una controversia tra una persona famosa e la stampa – il Supremo Collegio spiega che il “neo-diritto” consiste nella tutela di quelle situazioni personali e familiari, che non hanno un interesse socialmente apprezzabile per i terzi, contro le ingerenze non giustificate da interessi pubblici preminenti. In netto contrasto con i precedenti indirizzi, è affermato come la tutela riguardi i casi in cui l'intromissione nella vita privata avvenga «pure con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro»⁶ e lo stesso principio viene ribadito con i medesimi termini anche nella giurisprudenza successiva della Corte⁷.

Viene così pienamente riconosciuto nel nostro ordinamento il diritto alla riservatezza, seppur ancora in una forma riconducibile al “diritto ad essere lasciati soli”. Sarà necessario attendere il 1996 per la prima normativa in materia nel nostro ordinamento (L. n. 675/1996 poi rifluita nel D.Lgs. n. 196/2003), in ritardo rispetto a tutti i paesi dell'Unione Europea, eccetto la Grecia. Per fare un paragone, in

⁵ Cass. 20 aprile 1963, n. 990, *Petacci c. Palazzi e altri*, in *Il Foro Italiano*, Vol. 86, n. 5, 1963, p. 877-880.

⁶ Cass. 27 maggio 1975, n. 2129, *Soraya Esfandiari c. Soc. Rusconi editore; Soc. Rusconi editore c. Soraya Esfandiari*. Cassa App. Milano 19 gennaio 1971, in *Il Foro Italiano*, Vol. 99, 1976, p. 2895-2908.

⁷ Cass. 21 febbraio 1994, n. 1652, in *Rivista Giurisprudenza Italiana*, I, 1, 1995, p. 298.

Francia era già stato introdotto l'art. 9 al *Code Civil* sul «*droit à la vie privée*» nel 1970.

A livello sovranazionale viene firmata la *Convenzione per la protezione degli individui con riguardo al trattamento automatizzato di dati personali* (“Convenzione 108” o “Convenzione di Strasburgo”) nell’ambito del Consiglio d’Europa, aperta anche a Stati al di fuori dell’organizzazione e ratificata da 55 Paesi (in Italia, nel 1989) e, successivamente, anche dalla stessa Unione Europea nel 1999. Essa ha definito «le modalità e gli strumenti» della tutela per il diritto al rispetto della propria vita privata e familiare garantito già nella *Convenzione Europea dei Diritti dell’Uomo* (CEDU)⁸.

Il primo atto normativo di matrice comunitaria è invece la Direttiva 95/46/CE relativa alla «tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati» e, dopo diversi interventi legislativi, il quadro è stato ridefinito con il Regolamento (UE) 2016/679 che ha abrogato la previgente direttiva nel 2018. Parallelamente all’espansione di questo nuovo ordine di diritti, nella seconda metà del XX secolo avviene una diffusione su larga scala degli «elaboratori elettronici»⁹, meglio conosciuti come *computers*.

Il rapido sviluppo delle tecnologie informatiche, prima, e di quelle digitali, dopo, ha ampliato il concetto di tutela della riservatezza perché sono sorte nuove esigenze di protezione a fronte di pericoli ancor più grandi dell’aggressione dei mass media, come la facilità con cui le informazioni che riguardano ogni cittadino possano essere «tracciate e incrociate»¹⁰. A causa di questo mutamento, scrive *Stefano Rodotà*, «una definizione della privacy come diritto ad essere lasciato solo, come semplice riservatezza, ha da tempo perduto significato generale [...] La privacy, quindi, può in primo luogo, e più precisamente, essere definita come il diritto di mantenere il controllo sulle proprie informazioni»¹¹.

È nella società odierna che il diritto alla privacy acquisisce centralità negli ordinamenti moderni e solo uno sguardo poco consapevole guarderebbe a questo

⁸ MONTUORI L., *Privacy: perché la Convenzione 108+ è cruciale per il libero flusso dei dati*, in *Agendadigitale.eu*, Milano, 2022.

⁹ RODOTÀ S., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

¹⁰ GIOVANELLA F., PASCUZZI G., *Dal diritto alla riservatezza alla computer privacy*, in PASCUZZI G. (a cura di), *Il diritto dell’era digitale*, Il Mulino, Bologna, 2016, p. 47.

¹¹ RODOTÀ S., *Riservatezza*, in *Enciclopedia Italiana*, VI Appendice, Roma, 2000.

diritto come un semplice freno alla libertà e all'economia: in un mondo in cui la nuova merce di scambio – «[...] *the new currency of the digital world*»¹² – sono i dati personali, chi è più disposto a fornirli può ottenere maggiori servizi proprio come in un'arcaica società fondata sul censo era invece il patrimonio a creare discriminazioni tra gli individui. Da questo ulteriore punto di vista è possibile apprezzare maggiormente l'importante ruolo del *GDPR*, come difesa contro le discriminazioni del nuovo millennio.

Il nuovo Regolamento europeo 2016/679 sul trattamento dei dati personali entra in vigore a maggio 2016, vent'anni dopo la precedente Direttiva 95/46 che per anni ha delineato il quadro normativo della materia. Il legislatore italiano ha recepito la direttiva attraverso due atti interni, la legge n. 675/1996 sostituita poi dal d.lgs n. 196/2003 (“Codice della Privacy”). Durante il periodo di vigenza del primo atto sono intervenuti diversi fattori sul piano internazionale che hanno influito e orientato le scelte prese dal legislatore europeo.

Il primo fenomeno a cui fare riferimento è la «rapidità dell'evoluzione tecnologica» che ha influenzato la portata della condivisione e della raccolta di dati personali, « [...] aumentata in modo significativo»¹³, e che ha permesso a pochi gruppi imprenditoriali di gestire e trattare informazioni sugli individui con strumenti e modalità che fino a pochi anni fa risultavano impensabili – si usa l'acronimo OTT (*Over The Top*)¹⁴ per riferirsi alla posizione di predominanza del mercato assunta da queste aziende per le quali non risultano applicabili regole ordinarie. La loro prevalenza sul mercato si traduce, indirettamente, in un potere che esorbita dai limiti dello stesso e influisce anche sulle istituzioni e sulla politica.

Questo elemento non può essere scisso dalla considerazione, discussa più volte dagli operatori giuridici¹⁵, che queste grandi imprese hanno spesso sede negli Stati

¹² KUNEVA M., European Consumer Commissioner, *Roundtable on Online Data Collection, Targeting and Profiling, Bruxelles*, 31 marzo 2009.

¹³ Reg. (UE) 2016/679, Considerando 6.

¹⁴ NERVI A., *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 162 ss.

¹⁵ SARTOR G., VIOLA DE AZEVEDO CUNHA M., *Il caso Google e i rapporti regolatori USA/UE*, in *Diritto dell'Informazione e dell'Informatica*, 2014, 661.

Uniti D'America o, comunque, fuori dal territorio comunitario ed operano dunque sulla base di regole diverse da quelle stabilite nel mercato europeo.

Un altro fenomeno da considerare è quello della diffusione del terrorismo internazionale, problema entrato nella realtà di ogni paese occidentale a partire dall'11 settembre 2001. Alla necessità per gli Stati di adottare misure più efficaci e invadenti per garantire la sicurezza dei propri cittadini si contrappone il contrastante bisogno di tutelare i dati personali degli stessi. La tensione tra questi due principi si riflette su più livelli da oltre vent'anni ed è possibile individuarla in diverse sentenze, come ad esempio il recente caso *Schrems I* della Corte di Giustizia dell'Unione Europea che ha riorganizzato gli accordi UE-USA sul trasferimento dei dati personali verso Paesi terzi¹⁶ o la sentenza *Schrems II* che ha invalidato lo scudo per la privacy USA-UE (*Privacy Shield*) riconoscendo che la normativa americana non fornisce un livello di protezione equivalente a quello dell'Unione Europea¹⁷. La CGUE ha svolto un ruolo primario in questo tema e i suoi numerosi interventi non si sono limitati a decidere sul caso concreto ma hanno avviato un dialogo costante con il legislatore influenzandone le scelte.

Le differenze tra il Regolamento e la Direttiva, sul piano normativo, sono una conseguenza dei diversi valori che stanno alla base dell'approccio scelto per ciascuno dei due interventi del legislatore europeo. La direttiva venne adottata con l'obiettivo principale di uniformare le regole del mercato unico europeo in materia di trattamento di dati personali, eliminando le barriere nazionali alla loro circolazione e assicurando una disciplina uniforme. È difficile ritenere che questo fine sia stato raggiunto, a causa delle azioni discontinue, divergenti e frammentarie dei vari legislatori nazionali. Il risultato è stato quello di aver ottenuto una disciplina asimmetrica la cui conseguenza più evidente la si nota nel diverso ruolo che ogni paese ha riconosciuto ai Garanti della privacy (*Data Protection Authorities*), che in alcuni Stati membri sono stati previsti senza alcun potere sanzionatorio¹⁸. Nel «considerando» 9 del Regolamento, è lo stesso legislatore comunitario ad

¹⁶ C-362/14.

¹⁷ C-311/18.

¹⁸ PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Giuffrè Francis Lefebvre, Milano, 2019, p. 12 ss.

individuare i problemi sorti nell'applicazione della direttiva 95/46/CE che «non ha impedito la frammentazione dell'applicazione della protezione dei dati personali [...] né ha eliminato l'incertezza o la percezione [...] che [...] le operazioni online comportino rischi per la protezione delle persone fisiche»¹⁹ – non manca il riconoscimento di un «[...] divario creatosi nei livelli di protezione» che ha causato lo sviluppo di veri e propri «paradisi dei dati» nel mercato europeo²⁰.

Il secondo intervento del legislatore europeo ha una diversa finalità: l'attenzione si è spostata all'esterno dell'Europa e in particolare verso quei soggetti non europei che nelle loro attività coinvolgono cittadini dell'Unione – il fine è stato quello di rendere operanti le regole e i principi dell'ordinamento UE nei confronti di tali soggetti (i già citati *OTT*). Lo strumento della direttiva è stato abbandonato a favore di un atto di portata generale e di immediata esecutività, che ha permesso di disciplinare la materia attraverso un percorso comune a tutti gli Stati membri impedendo agli stessi di modificarne contenuti e forma se non attraverso atti di armonizzazione interni (in Italia, ad esempio, l'adeguamento alle disposizioni del Regolamento è avvenuto attraverso il d.lgs n. 101/2018).

Il fondamento del Regolamento sono gli artt. 7 e 8 della *Carta dei Diritti Fondamentali dell'Unione Europea*, che riconoscono, tra le libertà, il rispetto della vita privata e familiare («ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni») e la protezione dei dati di carattere personale («ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge; ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica; il rispetto di tali regole è soggetto al controllo di un'autorità indipendente»).

¹⁹ Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 - *Regolamento generale sulla protezione dei dati* (GDPR), Considerando 9

²⁰ PANETTA R. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, Giuffrè Francis Lefebvre, Milano, 2019, p. 7.

L'ambito di applicazione del GDPR è quello del «trattamento dei dati personali», la cui definizione è inserita nell'art. 4 e corrisponde quella presente nella Direttiva – «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»²¹. Questa definizione rende irrilevante l'ausilio o meno di processi automatizzati, tuttavia nell'art. 2 il legislatore restringe l'ambito di applicazione materiale riguardante il trattamento non automatizzato solo a quelli che riguardano «[...] dati personali contenuti in un archivio o destinati a figurarvi»²². Il concetto di archivio, per completare il quadro normativo delle definizioni, nel successivo art. 4 è illustrato come «qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati [...]»²³.

La disposizione comprende sia trattamenti automatizzati che manuali perché, chiarisce il Considerando 15, per evitare «gravi rischi di elusione, la protezione [...] non dovrebbe dipendere dalle tecniche impiegate»²⁴. Il legislatore europeo è consapevole della rapida mutevolezza delle tecnologie in questione e di come il ricorso a nuovi strumenti, ancora eventualmente estranei alla disciplina, porterebbe a una violazione *de facto* delle disposizioni previste – introduce dunque un concetto di «neutralità tecnologica»²⁵ la cui unica eccezione è rappresentata dal fatto che i dati debbano essere contenuti (o essere destinati a figurare) in un archivio che, definito in maniera così ampia, rende difficile immaginare un trattamento svolto al di fuori dello stesso. In questo modo, si contribuisce a rendere la portata del Regolamento, in maniera effettiva, “generale”.

Rimangono esclusi dall'applicazione del Regolamento i trattamenti di dati personali «effettuati da una persona fisica per l'esercizio di attività a carattere

²¹ Reg. (UE) 2016/679, art. 4, par. 1, n.2.

²² Reg. (UE) 2016/679, art. 2, par. 1.

²³ Reg. (UE) 2016/679, art. 4, lett. 6.

²⁴ Reg. (UE) 2016/679, Considerando 15.

²⁵ RICCIO G. M., SCORZA G., BELISARIO E. (a cura di), *GDPR e Normativa Privacy. Commentario*, Ipsoa, Roma, 2018, p. 12.

esclusivamente personale o domestico»²⁶. La delimitazione dell'ambito di questa tipologia di trattamento è fornita dalla Corte di giustizia²⁷ secondo cui è qualificabile come tale solo il trattamento che rimane confinato nella sfera giuridica del soggetto titolare senza interferire con quella altrui, il che non avviene «nel caso del trattamento di dati personali consistente nella loro pubblicazione su Internet in modo da rendere tali dati accessibili ad un numero indefinito di persone» – il Regolamento è dunque applicabile solo a quei trattamenti che, effettivamente o potenzialmente, generano una relazione giuridicamente rilevante tra il titolare ed un altro soggetto di diritto²⁸, indipendentemente dalle modalità con cui vengono effettuati. È possibile trovare una conferma di queste considerazioni nelle linee guida adottate dall'*European Data Protection Board*, che forniscono un'interpretazione restrittiva della deroga: tra gli esempi riportati, vi è quello di un turista che registra video per documentare le proprie vacanze mostrando il filmato ad amici e familiari senza renderli accessibili a un numero non definito di persone – sarebbe invece da escludere la qualificazione come attività personale o domestica per una registrazione che avviene attraverso sistemi di videosorveglianza della propria abitazione quando, come chiarito nelle linee guida, il filmato si estende anche in modo parziale a uno spazio pubblico o ad un'altra proprietà confinante²⁹.

Restano altresì esclusi i trattamenti che rientrano nelle attività di esclusiva competenze degli Stati membri, quali la sicurezza nazionale e la politica estera e di difesa comune dell'UE, nonché i trattamenti in ambito penale per finalità di indagine da parte delle autorità competenti³⁰.

Chiarito l'ambito materiale del Regolamento, è da riportare la sua più grande novità: essa risiede nell'ambito di applicazione territoriale, fondamentale carattere distintivo rispetto alla Direttiva per i motivi già citati. Per la prima volta, infatti, nella storia del diritto è stato messo radicalmente in discussione il principio di

²⁶ Reg. (UE) 2016/679, art. 2, par. 2, lettera c.

²⁷ C-101/01, *Bodil Lindqvist*, 6 novembre 2003, punto 47.

²⁸ NERVI A., *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in CUFFARO V., D'ORAZIO R., RICCIUTO V. (a cura di), *I dati personali nel diritto europeo*, G. Giappichelli Editore, Torino, 2019, p. 166.

²⁹ European Data Protection Board, *Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, adottate il 29 gennaio 2022, p. 8-9.

³⁰ Reg. (UE) 2016/679, art. 2, par. 2, lett. b, d.