PROF. AVV. MARCELLO CONDEMI

Professore Straordinario di Diritto dell'Economia nell'Università di Roma - G.Marconi
Dipartimento di Dipartimento di Scienze giuridiche e politiche
Facoltà di Giurisprudenza
Patrocinante dinanzi le Giurisdizioni Superiori ed Europee
Revisore Legale

Protezione dei dati di carattere personale e tutela risarcitoria

Sommario: 1. Evoluzione storico-normativa della disciplina in materia di privacy; 2. Il regime risarcitorio antecedente all'adeguamento della normativa nazionale al Regolamento generale sulla protezione dei dati ("G.D.P.R.)"; 2.1. Segue: Regime risarcitorio successivo all'adeguamento della normativa nazionale al Regolamento generale sulla protezione dei dati ("G.D.P.R."); 2.2. Segue: Segue: Condizioni necessarie ai fini della configurazione della responsabilità risarcitoria per danno derivante da violazione delle disposizioni del Regolamento generale sulla protezione dei dati (G.D.P.R.); 3. Privacy e Cybersecurity; 4. Conclusioni

1. *Evoluzione storico-normativa della disciplina in materia di privacy*

L'Unione Europea, pur affondando le proprie radici in un'organizzazione internazionale di stampo commerciale[1], si è evoluta nel corso dei decenni, fino a raggiungere un assetto organizzativo le cui caratteristiche, ad oggi, risultano essere un *unicum* a livello globale, non qualificandosi giuridicamente né come Stato, potenzialmente di tipo federale o confederale, in quanto è essa stessa composta da Stati sovrani, né come una mera organizzazione internazionale, attesi il particolare assetto dei poteri delle istituzioni europee, l'efficacia delle

[1] Cfr., sul tema, VILLANI, *Istituzioni di Diritto dell'Unione europea. IV edizione riveduta ed aggiornata*, Cacucci Editore, Bari, 2017, pagg. 4 ss. L'autore riporta che *«La prima organizzazione, con la quale ha inizio quel processo di integrazione europea, caratterizzato da un progressivo "trasferimento" di poteri sovrani da parte degli Stati membri a enti che, proprio in ragione della novità del fenomeno, vennero designati come "Comunità sopranazionali" (non più organizzazioni internazionali), è la Comunità europea del carbone e dell'acciaio (CECA) (…) I sei Stati giunsero così alla firma a Parigi, il 18 aprile 1951, del Trattato istitutivo della CECA, che entrato in vigore il 23 luglio 1952 (…) prevedeva, all'art. 97, un termine di durata di cinquant'anni dalla sua entrata in vigore. Esso, pertanto, ha perso efficacia il 23 luglio 2002 e la CECA si è estinta (…) Il rilancio del processo d'integrazione europea ebbe luogo nella Conferenza di Messina (…) e condusse alla firma a Roma, il 25 marzo 1957, del Trattato Istitutivo della Comunità economica europea (CEE) e di quello istitutivo della Comunità europea dell'energia atomica (CEEA o Euratom)».*

proprie fonti normative nei confronti degli Stati che la compongono e, anche, la previsione della cittadinanza europea, *a latere* di quella propria del Paese membro di origine.

Nel corso di tale evoluzione, oltre all'acquisizione di nuovi membri o alla definizione di una politica economica ovvero ancora, relativamente alla c.d. "Area Euro", di una politica monetaria comune, l'Unione si è distinta per il ruolo di primaria importanza esercitato a tutela dei diritti fondamentali dei propri cittadini, circostanza questa che trova la massima espressione nella Carta dei diritti fondamentali dell'Unione Europea (c.d. Carta di Nizza), firmata nel 2000 ed equiparata, ai sensi dell'art. 6, paragrafo 1, TUE[2], ai Trattati Istitutivi dell'Unione.

Nel quadro dell'azione europea di difesa dei diritti fondamentali, ruolo di prim'ordine viene riconosciuto al diritto alla protezione dei dati personali, c.d. diritto alla *privacy*, il quale, a livello "costituzionale"[3], viene sancito sia dall'art. 8 della Carta dei diritti fondamentali dell'Unione Europea[4], sia dall'art. 16 TFUE[5], mentre, nel quadro delle fonti eurounitarie di diritto derivato, trova

---

[2] *«L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati. Le disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni».*

[3] È necessario ricordare che l'Unione Europea non è dotata di una costituzione *stricto sensu*, atteso il fallimento, in termini politici, del progetto di creazione della stessa riconducibile alla posizione contraria assunta, in tale progetto, da Francia e Paesi Bassi nel 2005, con successivo abbandono da parte del Consiglio Europeo nel 2007. L'assenza di una costituzione in senso proprio non impedisce tuttavia di evidenziare come i valori riconosciuti all'interno dei Trattati e della Carta di Nizza siano investiti di un ruolo di primaria rilevanza, potendosi ravvisare in essi un rango sostanzialmente costituzionale.

[4] Recita l'art. 8 della Carta: *«Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano* (enfasi nostra). *2. 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. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».*

[5] Recita l'art. 16 TFUE: «*Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano* (enfasi nostra). *2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. 3. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea».*

riconoscimento e disciplina nel Reg. 679/2016 [*"Regolamento generale sulla protezione dei dati"* anche noto con l'acronimo di GDPR (*General Data Protection Regulation)*], che ha abrogato la Dir. 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*", provvedimento quest'ultimo che, per primo, ha disciplinato organicamente la materia a livello eurounitario.

L'emanazione del G.D.P.R. ha, invece, determinato l'adeguamento del quadro normativo italiano al nuovo impianto normativo attraverso il d.lgs. 10 agosto 2018, n. 101, recante, appunto, *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*, modificativo del d.lgs. 30 giugno 2003, n. 196 ["*Codice in materia di protezione dei dati personali"* (c.d. Codice della *Privacy*)], di recepimento della direttiva 95/46/CE.

2. Il regime risarcitorio antecedente all'adeguamento della normativa nazionale al Regolamento sulla protezione dei dati ("G.D.P.R.").

Il primo adeguamento della normativa nazionale alle disposizioni della Dir. 95/46/CE è avvenuto, come appena ricordato, a mezzo del summenzionato d.lgs. 196/2003, il quale, tra i molti, ha regolato il tema della responsabilità per danno derivante dalla violazione della disciplina in materia di protezione dei dati personali, mitigando il regime normativo di detta responsabilità al contenuto della disciplina comunitaria.

Quanto testé affermato è facilmente riscontrabile osservando il tenore letterale delle disposizioni di entrambi i citati provvedimenti normativi: infatti, se, da un lato, l'art. 23, par. 2, della Dir. 95/46/CE affermava che «(i)*l responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che*

l'evento dannoso non gli è imputabile» (riscontrandosi l'assenza di "imputabilità", ai sensi del considerando 55 della stessa, solo allorquando venga dimostrata «*l'esistenza di un errore della persona interessata o un caso di forza maggiore*»), dall'altro, l'art. 15 del d.lgs. 196/2003, nell'affrontare il tema dei "*danni cagionati per effetto del trattamento*", prevedeva che «*chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11*[6]».

Il richiamo all'art. 2050 c.c. - rubricato come "*Responsabilità per l'esercizio di attività pericolose*" ed ai sensi del quale «(c)*hiunque cagiona danno ad altri nello svolgimento di un'attivita' pericolosa, per sua natura o per la natura dei mezzi adoperati, e' tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno*» - comportava, *per tabulas*, la qualificazione dell'attività del trattamento dei dati personali quale "attività pericolosa", a cui conseguiva, ove non si fosse riusciti a provare di "*avere adottato tutte le misure idonee a evitare il danno*", un regime di imputazione della responsabilità per così dire rafforzato che, prescindendo dalla sussistenza dell'elemento soggettivo doloso o colposo richiesto dall'ordinario regime di responsabilità extracontrattuale di cui all'art. 2043 c.c.[7], si traduceva in una presunzione (*iuris tantum*) di responsabilità in capo al titolare del trattamento; tant'è che, secondo il consolidato orientamento della giurisprudenza di legittimità[8], «(l)*a presunzione di responsabilità contemplata dall'art. 2050 c.c. per attività pericolose può essere vinta solo con una prova*

[6] L'art. 11 del d.lgs. 196/2003 prevede che «(i) *dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalita' per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati».*

[7] L'art. 2043 c.c. precisa, in particolare, che «*Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno*».

[8] Cfr., sul punto, Cass. civ., Sez. VI, 19.5.2022, n. 16170, nonché, *ex multis*, Cass. civ., Sez. VI, 28.9.2021, n. 26236; Cass. civ. Sez. III, 21.2.2020, n. 4590; Cass. civ., Sez. III, 7.11.2019, n. 28626; Cass. civ., Sez. III, 22. 9.2014, n. 19872; Cass. civ., Sez. I, 28. 5. 2012, n. 8451.

particolarmente rigorosa, e cioè con la dimostrazione di aver adottato tutte le misure idonee ad evitare il danno: pertanto non basta la prova negativa (enfasi aggiunta) *di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva* (enfasi aggiunta) *di avere impiegato ogni cura o misura volta ad impedire l'evento dannoso, di guisa che anche il fatto del danneggiato o del terzo può produrre effetti liberatori solo se per la sua incidenza e rilevanza sia tale da escludere, in modo certo, il nesso causale tra attività pericolosa e l'evento e non già quando costituisce elemento concorrente nella produzione del danno, inserendosi in una situazione di pericolo che ne abbia reso possibile l'insorgenza a causa dell'inidoneità delle misure preventive adottate»*[9].

Pur nel suo incontestabile rigore, il disposto dell'art. 15 del d.lgs. 196/1993 risultava, tuttavia, più attenuato e blando rispetto alla disciplina contenuta nell'art. 23, par. 2, della Dir. 95/46/CE, potendosi, a tenore di quest'ultima, svincolare dalla responsabilità per danno esclusivamente qualora (i) il soggetto responsabile del trattamento avesse dimostrato di non essere coinvolto nella condotta che aveva determinato il prodursi dell'evento dannoso (condotta, invece, posta in essere dal diretto interessato) ovvero qualora (ii) fosse stata provata l'esistenza di una causa di forza maggiore.

In ambo i casi, si trattava, all'evidenza, di un rigoroso onere probatorio che, sebbene con difficoltà, consentiva comunque all'agente, in presenza dei necessari presupposti, di provare l'assenza di alcuna, propria responsabilità (c.d. "Responsabilità Oggettiva Spuria"); tale formula, sebbene rigorosa, evitava tuttavia che si ricadesse nel ben più stringente regime, meglio conosciuto come "Responsabilità Oggettiva Pura", che, a prescindere dall'accertamento dell'elemento soggettivo, dalla riprovevolezza della condotta e financo dal caso fortuito e dalla forza maggiore, imputa, sempre e comunque, all'agente la responsabilità di quanto accaduto[10].

[9] Cit. Cass. civ., Sez. VI, 19.5.2022, n. 16170.

[10] Con il termine "responsabilità oggettiva pura" (o propria), si fa riferimento, invero, ad una forma di responsabilità che, non lasciando spazio alcuno a qualsivoglia prova liberatoria, fa gravare in capo all'autore

La ragione della scelta, da parte del legislatore nazionale, di adottare un sistema più blando rispetto all'allora modello comunitario risiedeva, probabilmente, nell'inopportunità del recepimento di una formulazione nell'ordinamento nazionale (quale quella discendente dal combinato disposto dell'art. 23, par. 2, e del considerando 55 della Dir. 95/46/CE), nel quale, financo nelle ipotesi di più stringente responsabilità oggettiva c.d. "spuria" (la sola, d'altro canto, ammissibile nel nostro ordinamento), è sempre prevista in capo all'agente,

---

l'obbligo risarcitorio per il solo fatto di aver posto in essere la condotta collegata all'evento lesivo da nesso causale. Una responsabilità di tal guisa contrasterebbe, tuttavia, non solo con il tradizionale brocardo del "*nulla poena sine culpa*", ma anche (e soprattutto) con il dettato di cui all'art. 27, comma 1, Cost., laddove si prevede che "(l)*a responsabilità penale è personale*": difatti, specie in ambito penale, è necessario che sussista, oltre all'elemento soggettivo, un nesso causale o, quantomeno, che non si siano verificate condizioni, quali il caso fortuito o la forza maggiore, idonee per loro stessa natura ad interrompere il collegamento con la volontà dell'agente. Proprio con riferimento all'art. 27, comma 1, Cost., la responsabilità oggettiva pura è stata oggetto di esame da parte della Corte Costituzionale, la quale, con la storica sentenza n. 364/1988, ha affermato quanto segue. *«Ed anche a proposito dell'esclusione, nel primo comma dell'art. 27 Cost., del tassativo divieto di responsabilità oggettiva va precisato che (ricordata l'incertezza dottrinale in ordine alle accezioni da attribuire alla predetta espressione) se nelle ipotesi di responsabilità oggettiva vengono comprese tutte quelle nelle quali anche un solo, magari accidentale, elemento del fatto, a differenza di altri elementi, non è coperto dal dolo o dalla colpa dell'agente (c.d. responsabilità oggettiva spuria od impropria) si deve anche qui ribadire che il primo comma dell'art. 27 Cost. non contiene un tassativo divieto di "responsabilità oggettiva". Diversamente va posto il problema, a seguito di quanto ora sostenuto, per la c.d. responsabilità oggettiva pura o propria».* Di qui il riconoscimento, per converso, della responsabilità oggettiva, definita come "spuria" o "impropria", vale a dire di quella forma di responsabilità che, pur prevedendo un rilevante aggravamento in termini probatori della posizione dell'agente (dovendo il danneggiato solo provare il nesso causale, mentre il danneggiante, per via della prevista inversione dell'onere della prova, deve dimostrare la inapprensibilità della propria condotta), ammette comunque la prova liberatoria a favore dell'autore della condotta che ha determinato l'evento lesivo. Cass. civ., SS.UU., 21.05.2018, n.12477 precisa, in proposito, che «*la responsabilità oggettiva può infatti concepirsi solo laddove difetti un rapporto in senso lato "contrattuale" fra danneggiante e danneggiato, ed il primo sia chiamato a rispondere del fatto dannoso nei confronti del secondo non per essere con questi entrato in contatto, ma in ragione della particolare posizione rivestita o della relazione che lo lega alla res causativa del danno. Non a caso, dottrina e giurisprudenza hanno individuato ipotesi di responsabilità oggettiva nelle fattispecie tipiche delineate dagli artt. 2048 e 2053 c.c., tutte annoverabili nel più ampio genus dell'illecito extracontrattuale».* Nel contesto giurisprudenziale, quindi, la "responsabilità oggettiva" indica una forma di responsabilità oggettiva di tipo "spurio", attesa l'impossibilità di configurare nel nostro ordinamento, alla luce dell'art. 27, comma 1, Cost. (da assumersi quale parametro generale di imputazione della responsabilità in generale), alcuna forma di responsabilità oggettiva, c.d. "pura", il cui obbligo risarcitorio sarebbe collegato al solo fatto di aver posto in essere la condotta collegata all'evento lesivo da nesso causale [cfr., in ordine alla nozione di responsabilità oggettiva, Trib. Trento, 11.09.2015, n.863, secondo cui «(n)*e deriva l'applicabilità dell'art. 2050 c.c., che fonda un'ipotesi di responsabilità presunta o oggettiva, in base alla quale, il danneggiante può liberarsi da responsabilità, solo offrendo la prova di aver adottato tutte le cautele idonee ad evitare il danno*»; Trib. Torino, Sez. I, 06.06.2022, n.2451, a mente della quale «(p)*er i danni causati dal promotore di prodotti finanziari o assicurativi risponde anche la banca ex art. 2049 c.c.: infatti la predetta norma delinea una fattispecie di responsabilità oggettiva per il danno provocato dal proprio incaricato, danno reso possibile o agevolato dalle incombenze demandategli, a patto che il committente abbia avuto la possibilità di esercitare poteri di direttiva e di vigilanza. La sua configurabilità, dunque, prescinde dalla forma del rapporto essendo sufficiente che il commesso abbia agito per conto e sotto la vigilanza del committente»;* Cass. civ., Sez. III, 08.02.2023, n.3739, ad avviso della quale «(l)*a responsabilità ex art. 2051 c.c. postula la sussistenza di un rapporto di custodia della cosa e la relazione di fatto tra un soggetto e la cosa stessa, tale da consentire il potere di controllarla, di eliminare le situazioni di pericolo che siano insorte e di escludere i terzi dal contatto con la cosa; ad integrare la responsabilità è necessario e sufficiente che il danno sia stato "cagionato" dalla cosa in custodia, assumendo rilevanza il solo dato oggettivo della derivazione causale del danno dalla cosa sicché il danneggiato ha il solo onere di provare l'esistenza di un idoneo nesso causale tra la cosa e il danno, mente al custode spetta di provare che il danno non è stato causato dalla cosa ma dal caso fortuito nel cui ambito sono compresi, oltre al fatto naturale, anche quello del terzo e dello stesso danneggiato; si tratta dunque di una responsabilità oggettiva con possibilità di prova liberatoria, nel cui ambito il caso fortuito interviene come elemento idoneo ad elidere il nesso causale altrimenti esistente tra la cosa e il danno*»].

seppure implicitamente, la possibilità di svincolarsi dall'obbligo risarcitorio dimostrando, da un lato, di non aver posto in essere la condotta da cui è scaturito l'evento lesivo, dall'altro, la sussistenza del caso fortuito o della forza maggiore[11]. L'applicazione di entrambe le richiamate esimenti, pur in assenza di una loro esplicita menzione da parte dell'art. 2050 c.c., è dettata dalla necessità di evitare che possa configurarsi un'ipotesi di responsabilità oggettiva pura, come noto inammissibile nel nostro ordinamento, rappresentando il caso fortuito «*quell'avvenimento imprevisto ed imprevedibile che si inserisce d'improvviso nell'azione del soggetto, e non può in alcun modo, nemmeno a titolo di colpa, farsi risalire all'attività psichica dell'agente*»[12] e postulando la forza maggiore «*l'esistenza di una vis maior cui resisti non potest, cioè di un evento derivante dalla natura o dal fatto dell'uomo che non può essere preveduto, o che, anche se preveduto, non può essere impedito*»[13].

2.1 <u>*Segue: Tutela risarcitoria successiva all'adeguamento della normativa nazionale al Regolamento sulla protezione dei dati ("G.D.P.R.").*</u>

L'emanazione del G.D.P.R. e il successivo adeguamento allo stesso da parte della normativa nazionale ha comportato, come noto, una profonda rimeditazione del previgente assetto normativo contenuto nel "Codice della *Privacy*": tra i molteplici profili oggetto di tale rimeditazione merita menzione, per quanto qui d'interesse, l'istituto della responsabilità per violazione delle disposizioni in materia di protezione dei dati personali. A mente dell'art. 27, comma 1, del d.lgs. 101/2018 vengono infatti «(…) *abrogati i titoli, capi, sezioni, articoli e allegati del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003* (Codice della Privacy), *di seguito elencati: a) alla parte I: 1) gli articoli 3, 4, 5 e 6; 2) il titolo II, il titolo III, il titolo IV, il titolo V, il titolo VI e il titolo VII (…)*». In particolare, all'interno dell'abrogata parte I, titolo III, era contenuto proprio il predetto art. 15 del Codice della Privacy in materia di responsabilità per danno

[11] La direttiva 196/1993 prevedeva, come noto, la sola "forza maggiore".
[12] Cit. Cass. pen., Sez. IV, 31 maggio 1990, n. 7825.
[13] Cit. Cass. pen., Sez. VI, 22 gennaio 1980, n. 1018

derivante da violazioni del G.D.P.R., la cui disciplina, adesso, risulta essere contenuta nell'art. 82 del Reg. 679/2016, ai sensi del quale «(*c*)*hiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento* (enfasi aggiunta). *2. Un titolare del trattamento*[14] *coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento* (enfasi aggiunta). *Un responsabile*[15] *del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento* (enfasi aggiunta). *3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile* (enfasi aggiunta). *4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno* (enfasi aggiunta)*, al fine di garantire il risarcimento effettivo dell'interessato. 5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2* (enfasi aggiunta). *6. Le azioni legali per l'esercizio*

[14] Ai sensi dell'art. 4, paragrafo 1, n. 7), del G.D.P.R. è definito "titolare del trattamento" «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*».

[15] Ai sensi dell'art. 4, paragrafo 1, n. 8, del G.D.P.R. è definito "responsabile del trattamento" «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*».

del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2[16]».

Orbene, dalla lettura dell'art. 82 del Regolamento, rispetto al sistema previsto dal previgente art. 15 del Codice della Privacy, a parte la diversa formulazione utilizzata ai fini dell'esclusione della imputabilità dell'evento dannoso ["*se non prova di avere adottato tutte le misure idonee a evitare il danno"* ex art. 2050 c.c. ovvero, ex art. 82 del Regolamento, "***se dimostra che l'evento dannoso non gli è in alcun modo imputabile"***], emergono molteplici differenze, quali, tra le altre:

1. la definizione, ai sensi dei commi 4 e 5, del regime applicativo della responsabilità in solido e del diritto di regresso sui coautori dell'illecito;
2. la differente posizione soggettiva del "titolare" e del "responsabile del trattamento" quali unici responsabili (sebbene a diverso titolo ed in luogo della locuzione "chiunque" contenuta nell'art. 15 del Codice della Privacy) dei danni causati dalla mancata protezione dei dati personali.

Quanto al tenore letterale del nuovo regime di responsabilità risarcitoria, occorre interrogarsi se, e nell'affermativa, in che misura, il mutato disposto normativo abbia modificato il previgente regime disciplinare della responsabilità per danni derivanti dal trattamento dei dati personali. Ferma la qualificazione della responsabilità di che trattasi, anche in presenza dell'attuale regime, quale "responsabilità oggettiva spuria", l'attuale formulazione – pur contenendo una precisazione assimilabile a quella contenuta nel considerando 55 della Dir. 95/46/CE, ma, nello stesso tempo, più ampia, dal momento che l'agente «(…) *è esonerato dalla responsabilità* (…) *se dimostra che l'evento dannoso non gli è in alcun modo imputabile*» - risulta essere, rispetto alla precedente, di più incerta

[16] L'art. 79, par. 2, del G.D.P.R. dispone quanto segue. *«Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri».*

ricostruzione, attesa l'assenza di un espresso rinvio ad alcun articolo di legge (circostanza, questa, ragionevolmente legata alla matrice eurounitaria della disposizione normativa applicabile a tutti i ventisette Paesi.

Di qui l'esigenza, pur nella certezza di spaziare all'interno della categoria della responsabilità oggettiva c.d. "spuria", di definire sulla base di quali parametri e strumenti sia possibile dimostrare che l'evento dannoso non sia "*in alcun modo imputabile*" all'agente: se cioè tale dimostrazione sia possibile fornirla a prescindere dalla circostanza, di cui al precedente assetto normativo, che egli abbia o meno "*adottato tutte le misure idonee a evitare il danno"* o se invece, in base ad una diversa (e più stringente) lettura del nuovo disposto regolamentare, ad escludere la responsabilità ed il conseguente addebito risarcitorio non basti dimostrare l'aver «*adottato tutte le misure idonee a evitare il danno*», ma la totale estraneità alla commissione dell'evento dannoso per assenza di nesso causale tra la condotta e l'evento lesivo.

Tale ultimo approccio interpretativo, tuttavia, alla luce di quanto già *supra* asserito, deve ritenersi di difficile praticabilità, posta l'inammissibilità del regime di "responsabilità oggettiva pura", poiché in contrasto con i principi del nostro ordinamento e, secondo l'insegnamento della Corte Costituzionale, con l'art. 27, comma 1, Cost.

Una possibile, diversa lettura dell'art. 82 del G.D.P.R., che consenta l'applicazione delle limitazioni probatorie già previste dall'art. 2050 c.c., eviterebbe, pur nel mutato regime, soluzioni di continuità con il precedente dettato dell'art. 15 del Codice della Privacy: un recente approdo giurisprudenziale di legittimità «(…) *condiviso anche dal Tribunale di Latina e conforme agli indirizzi di questa Corte (da ultimo Sez. 1, n. 207 del 8/1/2019), riconduce l'illecito trattamento di dati personali ad un'ipotesi di responsabilità oggettiva, anche alla luce dell'esplicito rinvio compiuto dalla legge (D.Lgs. n. 196 del 2003, art. 15 applicabile pro tempore) all'art. 2050 c.c.. Pertanto, il danneggiato che lamenti la lesione dell'interesse non patrimoniale può limitarsi a dimostrare l'esistenza del danno e del*

nesso di causalità rispetto al trattamento illecito, mentre spetta al danneggiante titolare del trattamento, eventualmente in solido col responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno. Questo schema è parzialmente confermato (enfasi aggiunta) *anche nel nuovo GDPR (art. 82.3 GDPR) che, sulla base del principio di responsabilizzazione (accountability) addossa al titolare del trattamento dei dati - eventualmente in solido con il responsabile - il rischio tipico di impresa (art. 2050 c.c.).*(…) *Il titolare del trattamento, per non incorrere in responsabilità deve dimostrare che l'evento dannoso non gli è in alcun modo imputabile e non può limitarsi alla prova negativa di non aver violato le norme (e quindi di essersi conformato ai precetti), ma occorre la prova positiva di aver valutato autonomamente il rischio di impresa, purché tipico, cioè prevedibile, e attuato le misure organizzative e di sicurezza tali da eliminare o ridurre il rischio connesso alla sua attività*»[17]. Ipotesi interpretativa, questa, sufficientemente appagante, per un verso, perché l'art. 82, par. 3, del Reg. 679/2016 si limita a precisare che «*3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile* (enfasi aggiunta)», per altro verso, perché dal tenore letterale dell'intero testo dell'art. 82 del G.D.P.R., non è dato cogliere alcuna precisazione, fortemente limitativa, di tenore analogo a quella presente nel considerando 55 dell'abrogata Dir. 95/46/CE (secondo cui l'imputabilità sarebbe stata esclusa solo allorquando fosse stata dimostrata «*l'esistenza di un errore della persona interessata o un caso di forza maggiore*»), con ciò lasciando all'elaborazione, dottrinale e giurisprudenziale, il compito di suggerire, com'è accaduto con l'orientamento sopra ricordato, una lettura regolamentare in linea con le caratteristiche e i principi a cui è informato l'ordinamento nazionale.

2.2 Segue: Condizioni necessarie ai fini della configurazione della responsabilità risarcitoria per danno derivante da violazione delle disposizioni del Regolamento sulla protezione dei dati (G.D.P.R.).

[17] Cit. Cass. civ., Sez. I, 17.09.2020, n. 19328.

La rilevanza della tematica qui affrontata è confermata anche dalla recente sentenza della Corte di Giustizia dell'Unione Europea, datata 4 maggio 2023, chiamata ad individuare le condizioni necessarie ai fini della giuridica configurazione di una ipotesi di responsabilità risarcitoria per danno derivante da violazione delle disposizioni del G.D.P.R. La Corte, adita in via pregiudiziale, ha esaminato, in tale quadro, le seguenti questioni: i) «*Se ai fini del riconoscimento di un risarcimento ai sensi dell'articolo 82 del RGPD occorra, oltre a una violazione delle disposizioni del RGPD, che il ricorrente abbia patito un danno, o se sia già di per sé sufficiente la violazione di disposizioni del RGPD per ottenere un risarcimento; (ii) Se esistano, per quanto riguarda il calcolo del risarcimento, altre prescrizioni di diritto dell'Unione, oltre ai principi di effettività e di equivalenza; (iii) Se* (infine) *sia compatibile con il diritto dell'Unione la tesi secondo cui il presupposto per il riconoscimento di un danno immateriale è la presenza di una conseguenza o di un effetto della violazione di un diritto avente almeno un certo peso e che vada oltre l'irritazione provocata dalla violazione stessa.*»

Relativamente alla prima questione, la Corte – prendendo le mosse dal tenore del paragrafo 1 *dell'articolo 82 del RGPD* [secondo cui *"(c)hiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento"*] ritiene tuttavia necessaria l'esistenza, cumulativa, di «(…) *di un "danno" che sia stato "subito"* (…)», «(…) *di una violazione del RGPD e di un nesso di causalità tra tale danno e tale violazione* (…)» – affermando, in conclusione, che «*non si può ritenere che qualsiasi "violazione" delle disposizioni del RGPD conferisca, di per sé, detto diritto al risarcimento a favore dell'interessato, come definito all'articolo 4, punto 1, del regolamento in esame* (…)» e che una diversa interpretazione si porrebbe «*in contrasto con il tenore letterale dell'articolo 82, paragrafo 1, di detto regolamento. D'altro lato* (prosegue la Corte) *occorre sottolineare che la menzione distinta di un "danno" e di una "violazione", all'articolo 82, paragrafo 1, del RGPD, sarebbe superflua se il legislatore dell'Unione avesse ritenuto che una violazione delle disposizioni del*

regolamento in parola possa essere sufficiente, da sola e in ogni caso, a dare fondamento a un diritto al risarcimento».

Con riguardo alla seconda questione, la Corte ha dichiarato che «*l'articolo 82 del RGPD deve essere interpretato nel senso che, ai fini della determinazione dell'importo del risarcimento dovuto in base al diritto al risarcimento sancito da tale articolo, i giudici nazionali* (in mancanza di norme dell'Unione in materia) *devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario, purché siano rispettati i principi di equivalenza* (*id est*: non siano meno favorevoli rispetto a quelle relative a situazioni analoghe assoggettate al diritto interno) *e di effettività del diritto dell'Unione* (*id est*: non rendano in pratica impossibile o eccessivamente difficile l'esercizio dei diritti conferiti dal diritto dell'Unione)»; e ciò in quanto «*il RGPD non contiene disposizioni intese a definire le norme relative alla valutazione del risarcimento danni che un interessato, ai sensi dell'articolo 4, punto 1, del regolamento di cui trattasi, può pretendere, in forza dell'articolo 82 di quest'ultimo, qualora una violazione di detto regolamento gli abbia causato un danno* (…) ed «(…) *in mancanza di norme del diritto dell'Unione in materia, spetta all'ordinamento giuridico di ciascuno Stato membro stabilire le modalità delle azioni intese a garantire la tutela dei diritti spettanti ai singoli in forza di detto articolo 82 e, in particolare, i criteri che consentono di determinare l'entità del risarcimento dovuto in tale ambito, fatto salvo il rispetto dei suddetti principi di equivalenza e di effettività».*

La Corte, infine, in relazione alla terza ed ultima questione, ha affermato, (i) in primo luogo, che «*il RGPD non definisce la nozione di «danno», ai fini dell'applicazione di tale strumento. L'articolo 82 di quest'ultimo si limita ad enunciare in modo esplicito che può dare diritto a un risarcimento non solo un «danno materiale», ma anche un «danno immateriale», senza che vega menzionata una qualsivoglia soglia di gravità* (…); (ii) in secondo luogo, che «(…) *il contesto in cui si inserisce tale disposizione tende altresì ad indicare che il diritto al risarcimento non è subordinato al fatto che il danno di cui trattasi raggiunga una certa soglia di gravità*», e ciò in quanto «*il considerando 146 del RGPD, alla terza frase, enuncia che "il concetto di danno*

dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del [suddetto regolamento]". Orbene (prosegue la Corte) *tale concezione ampia della nozione di "danno", privilegiata dal legislatore dell'Unione, sarebbe contraddetta se detta nozione fosse circoscritta ai danni di una certa gravità*». Una siffatta interpretazione, d'altra parte, risulta essere «*avvalorata dalle finalità perseguite dal RGPD*», dovendosi a tale riguardo, per un verso, rammentare «*che il considerando 146, terza frase, di tale regolamento invita espressamente a interpretare il concetto di "danno", ai sensi di quest'ultimo, in modo tale da rispecchiare "pienamente gli obiettivi del [suddetto] regolamento]*» e, per altro verso, rilevare che «*subordinare il risarcimento di un danno immateriale a una certa soglia di gravità rischierebbe di nuocere alla coerenza del regime istituito dal RGPD, poiché la graduazione di una siffatta soglia, da cui dipenderebbe la possibilità o meno di ottenere detto risarcimento, potrebbe variare in funzione della valutazione dei giudici aditi*».

3. <u>*Privacy e Cybersecurity*</u>

Data la strettissima correlazione con la protezione dei dati personali, si ritiene d'interesse, in un'ottica risarcitoria, fare brevi cenni alla tematica, anch'essa di

derivazione europea[18], della Cybersicurezza[19] [20]: la necessità di garantire una vera e propria protezione dei dati di cui il titolare viene in possesso non passa

[18] La prima normativa di rilievo nella prospettiva della cybersicurezza è la Direttiva Ue 2016/1148, anche nota come "Direttiva NIS", la quale evidenzia come l'Ue sia perfettamente conscia del fatto che «*Le reti e i sistemi e servizi informativi svolgono un ruolo vitale nella società. È essenziale che essi siano affidabili e sicuri per le attività economiche e sociali e in particolare ai fini del funzionamento del mercato interno*» (cit. Considerando 1 della direttiva) e che «*le reti e i sistemi informativi, e in prima linea internet, svolgono un ruolo essenziale nell'agevolare i movimenti transfrontalieri di beni, servizi e persone*» (cit. Considerando 3 della direttiva). Contemporaneamente nella direttiva si configura anche il grave pericolo che *«Tenendo conto di questa dimensione transnazionale, gravi perturbazioni di tali sistemi, intenzionali o meno e indipendentemente dal luogo in cui si verificano, possono ripercuotersi su singoli Stati membri e avere conseguenze in tutta l'Unione»* (cit. *Ibidem)*, con la conseguenza che *«La sicurezza delle reti e dei sistemi informativi è quindi essenziale per l'armonioso funzionamento del mercato interno*» (cit. *Ibidem*). Emerge, dunque, con chiarezza la *ratio* che ha condotto l'UE ad adottare una serie di *«misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno*» (cit. art. 1 della direttiva) che sono elencate al comma 2 dell'art. 1 Dir. 2016/1148, ai sensi del quale *«A tal fine la presente direttiva: a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; b) istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi; c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente («rete CSIRT») per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti connessi alla sicurezza della rete e dei sistemi informativi».* Tuttavia, in chiave critica, è necessario sottolineare come la direttiva in oggetto, limitandosi ad imporre agli Stati un generico obbligo di adozione di strategie nazionali di cybersicurezza, non abbia anche dettato i criteri da seguire a presidio dell'azione di contrasto, favorendo, in tal modo, l'assenza, nel quadro europeo, di un impianto armonizzato in materia di cybersicurezza.

[19] Termine, questo, che l'art. 1, comma 1, lett. a), del d.l. 14 giugno 2021, n. 82, recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"*, definisce come *«l'insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico».*

[20] Il diritto che funge da contraltare rispetto alla cybersicurezza è, come intuibile, la protezione dei dati personali, configurandosi, in tal modo, una sorta di rivalità insanabile tra l'Autorità per la Cybersicurezza Nazionale (ACN) ed il Garante per la Protezione dei Dati personali (GPDP), rivalità, tuttavia, solo apparente, non foss'altro perché entrambe le Autorità, in quanto pubbliche, risultano perseguire finalità di interesse collettivo. Infatti, come da un lato non potrebbe dirsi esistente qualsivoglia diritto di libertà ove non fossero garantiti contestualmente la sicurezza e l'ordine pubblico, dall'altro non potrebbe dirsi effettivo il diritto alla Protezione dei Dati personali in un contesto di totale assenza di cybersicurezza. Quanto appena affermato trova d'altra parte conferma nella circostanza che, ove l'ACN non operasse al fine di potenziare le misure di sicurezza cibernetica e, altresì, al fine di rafforzare la resilienza delle infrastrutture digitali, si rischierebbe di dover assistere, sul piano della Protezione dei Dati personali, a scenari non proprio rassicuranti. È sufficiente pensare, infatti, alle innumerevoli banche dati, pubbliche o private che siano, oggetto, per le finalità più disparate, di potenziali aggressioni cybernetiche, potendosi, in taluni casi, anche mettere a repentaglio la sicurezza nazionale. Si evince dunque, molto chiaramente, come il diritto alla Protezione dei Dati personali, oggi più che mai, non si limiti ad una mera dimensione individuale, ma si estenda fino a ricomprendere il più alto livello collettivo-nazionale: la sempre più rapida digitalizzazione, infatti, ha posto fuori dal controllo delle Autorità Nazionali ed Internazionali la odierna principale infrastruttura attraverso cui transitano i dati personali, rappresentata dal web, ed in particolar modo, dai *social network*. Ad ulteriore riprova dell'intima connessione tra *Cybersecurity* e *data protection*, è possibile citare l'avvertita necessità di apprestare, nel quadro della tutela dei dati personali, un approccio sinergico da parte dell'Autorità per la Cybersicurezza Nazionale (ACN) e del Garante per la Protezione dei Dati personali (GPDP), tanto che, in data 26 gennaio 2022, è stato firmato tra le stesse un Protocollo d'intesa che

esclusivamente attraverso le previsioni del GDPR, quanto anche (specie alla luce della incessante diffusione ed evoluzione delle tecnologie ad essa applicate), attraverso la *data protection* offerta dai sistemi di sicurezza informatica dei titolari e responsabili nei confronti di possibili incursioni *hacker* e *data breach*, sempre più frequenti ed aggressive[21], in danno, senz'alcuna distinzione, di infrastrutture digitali pubbliche e di istituzioni private d'impresa[22].
Il collegamento tra la sicurezza dei sistemi informatici e la tutela dei dati personali si può spiegare anche attraverso il grande valore economico che questi ultimi rivestono nell'attuale contesto economico globale, specie in ragione del loro peso commerciale e politico[23].

---

vede entrambe le Autorità unite per garantire i diritti dei cittadini e la tutela della sicurezza nazionale nello spazio cibernetico. Tale Protocollo garantisce l'avvio della cooperazione tra le due istituzioni, promuovendo iniziative congiunte nel campo della cybersicurezza nazionale e della protezione dei dati personali. Il Protocollo assicurerà agevoli interlocuzioni tra il Garante e l'ACN, segnatamente attraverso lo scambio di informazioni e la promozione di *best practice* di sicurezza cibernetica, permettendo all'Agenzia di consultare, fin dalla fase di avvio delle proprie attività, il Garante sui temi attinenti al trattamento dei dati personali, ed obbligando il Garante di informare l'Agenzia circa le rilevanti notizie di *data breach* a fini della cybersicurezza del Paese.
Il Protocollo avrà durata biennale, con la possibilità di essere rinnovato tacitamente e con il riconoscimento ad entrambe le parti di proporre aggiornamenti qualora le innovazioni normative e regolamentari dovessero richiederlo. Significative, al riguardo, sono state le dichiarazioni tanto del Presidente del GPDP Pasquale Stanzione, quanto quelle del Direttore generale dell'ACN Roberto Baldoni, affermando, rispettivamente, che *«La sigla del protocollo d'intenti rappresenta un momento molto importante per la tutela dei dati personali e della stessa cybersecurity nel nostro. Si attua, così, una previsione particolarmente lungimirante della disciplina istitutiva dell'Agenzia, laddove delinea nella cooperazione con il Garante uno dei punti qualificanti della strategia di tutela della cybersicurezza. L'applicazione del protocollo dimostrerà come questa collaborazione rappresenti una preziosa opportunità per la governance del digitale, nel segno del necessario equilibrio tra libertà e sicurezza sotteso all'art. 6 della Carta di Nizza»* e che «*La cybersicurezza del nostro mondo digitale, a cui è preposta l'Agenzia, è un'attività partecipata che non può che essere svolta in stretta cooperazione con le istituzioni, i cittadini e le imprese. È importante che ognuno, per il raggiungimento dei livelli adeguati di resilienza del Paese richiesti dal ritmo incalzante della trasformazione digitale che aumenta continuamente la superficie d'attacco, faccia la sua parte. La sigla del protocollo d'intenti promuove una virtuosa collaborazione, nel rispetto delle competenze del Garante, con una delle istituzioni più importanti nel nostro Paese, che permetterà uno scambio informativo di fondamentale importanza per garantire lo sviluppo digitale del Paese e il rispetto dei diritti fondamentali».*

[21] Secondo l'ultimo rapporto CLUSIT, *«*(n)*el 2020 gli attacchi con impatto "Critico" rappresentavano il 14% del totale, quelli di livello "Alto" il 36%, quelli di livello "Medio" il 32% ed infine quelli di livello "Basso" il 19%. Complessivamente, gli attacchi gravi con effetti molto importanti (High) o devastanti (Critical) nel 2020 erano il 50% del campione. Nel 2021 la situazione è molto diversa e francamente impressionante: gli attacchi gravi con effetti molto importanti (High) sono il 47%, quelli devastanti (Critical) rappresentano il 32%, quelli di impatto significativo (Medium) il 19%, e quelli con impatto basso solo il 2%. In questo caso gli attacchi con impatto Critical e High sono il 79%».*

[22] Le aggressioni, mirate a colpire la *supply chain* (*id est:* la catena di distribuzione) di imprese di interesse nazionale ovvero di PPAA, pur risultando, per ovvie ragioni, più complesse ciberneticamente rispetto a quelle da muovere nei confronti di un privato cittadino, appaiono essere tuttavia più attrattive e, anche, potenzialmente più profittevoli.

[23] A tale riguardo è possibile, a titolo esemplificativo, fare riferimento alla vicenda "Cambridge Analytica". Quest'ultima, fondata nel 2013 con lo scopo ultimo di occuparsi delle strategie di comunicazione politica per

La conseguenza più immediata è che banche dati di dimensioni rilevanti, quali quelle delle Pubbliche Amministrazioni o di enti creditizi e/o finanziari, rappresentano bersagli estremamente appetibili per i professionisti del *cybercrime*, i quali, non solo potrebbero rivendere le informazioni ottenute a terzi, ma, come sempre più frequentemente accade, potrebbero estorcere denaro tanto per la "restituzione" dei dati sottratti, quanto per liberare da vincoli, da essi apposti, i sistemi informatici dell'ente[24]. In aggiunta, è necessario sottolineare come, in una società sempre più digitalmente interconnessa, sia piuttosto semplice, da parte dei professionisti del *cybercrime*, arrecare danni, partendo dalla sottrazione dei dati di singoli soggetti privati, a soggetti strategicamente rilevanti per l'interesse nazionale, definiti, dall'art. 3 del d.lgs. 65/2018, "(o)*peratori di servizi essenziali*", vale a dire «*soggett(i) pubblic(i) o privat(i), della tipologia di cui all'allegato II*[25]*, che soddisfa i criteri di cui all'articolo 4, comma 2*[26]». Di qui le ragioni della prevista vigilanza sull'adeguatezza della sicurezza informatica dei sistemi degli operatori di servizi essenziali, da parte della nuova

finalità elettorali, quale filiale della società britannica SCL Group, si occupava prevalentemente di *big data* e *data mining*, Essa, attraverso l'esercizio di dette attività, aveva sintetizzato vari modelli comportamentali-psicologici relativi alle diverse tipologie di utenti che navigavano in rete. La divisione di Cambridge Analytica – che è stata artefice di plurime campagne elettorali in molteplici Paesi (tra cui quella presidenziale di Donald Trump nel 2016 e, nello stesso anno, quella *pro-Brexit*) - è stata resa celebre per via di un enorme scandalo relativo alla commercializzazione dei dati personali.

[24] La maggior parte delle incursioni risulta condotta attraverso *ransoware,* vale a dire attraverso una specifica tipologia di virus che rende inaccessibili i file dei *device* infettati, al fine di richiedere, in cambio del loro ripristino, utilità di vario genere (denaro, criptovalute, etc.): così facendo, il *cybercrime* riesce a finanziarsi adeguatamente potenziando il proprio potenziale aggressivo cibernetico ed instaurando un vero e proprio circolo vizioso di incursioni sempre più devastanti seguiti da riscatti sempre più elevati. Secondo quanto affermato dal "*Rapporto Clusit 2022 sulla sicurezza ICT in Italia*", nell'anno 2018 l'utilizzo di *ransomware* rappresentava il 23% dei complessivi *malware*, nel 2019 raggiungevano il 46%, nel 2020 arrivavano al 67% con un numero di 220 attacchi, mentre nel 2021 la misura arrivava quasi al 75%. Lo stesso Rapporto afferma che *«il C.N.A.I.P.I.C.* (*Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche), ha gestito 256 eventi ransomware (contro i 220 del 2020), di cui 61 contro Infrastrutture Critiche (IC), Operatori di Servizi Essenziali (OSE) e Piccole Amministrazioni Locali (PAL) e 195 attacchi ad aziende».*

[25] L'allegato prende in considerazione i seguenti settori: a) Energia [1. Energia Elettrica, 2. Petrolio, 3. Gas]; b) Trasporti [1. Trasporto aereo, 2. Trasporto ferroviario, 3. Trasporto via acqua, 4. Trasporto su strada]; c) Settore bancario; d) Infrastrutture dei mercati finanziari; e) Settore Sanitario; f) Forniture e distribuzione di acqua potabile; g) Infrastrutture digitali.

[26] I criteri per l'identificazione degli operatori di servizi essenziali sono i seguenti: a) un soggetto fornisce un servizio che e' essenziale per il mantenimento di attivita' sociali e/o economiche fondamentali; b) la fornitura di tale servizio dipende dalla rete e dai sistemi informativi; c) un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

Agenzia per la Cybersicurezza Nazionale (ACN), istituita ai sensi degli artt. 5-9 del d.l. 82/2021 (convertito, con modificazioni, nella L. 4 agosto 2021, n. 109), che si concretizza in attività di matrice consulenziale, ispettiva e sanzionatoria. Da quanto suesposto si evince, dunque, che in caso di attacco cibernetico da cui derivino eventi lesivi in capo ad un soggetto a causa della sottrazione dei propri dati personali, sulla banca dati graverebbe contestualmente tanto la responsabilità di matrice amministrativa, quanto quella di matrice civilistica, con la conseguente, possibile previsione, rispettivamente, dell'irrogazione di sanzioni amministrative pecuniarie e della condanna al risarcimento dei danni arrecati.

4. <u>Conclusioni</u>

La tematica della protezione dei dati personali si attesta oggi come una delle aree di maggior interesse e con le più ampie prospettive di evoluzione, non solo in ragione della natura intimamente connessa allo sviluppo delle nuove tecnologie, bensì anche in ragione della elevata sensibilità sociale maturata verso siffatta tematica, legata principalmente alla grande attenzione riservata (e alla pervasività dei presidi normativi apprestati) dall'Unione Europea.

Di qui il brevissimo passo verso la connessa tematica della tutela civilistica (e non solo) da riconoscere al danneggiato in conseguenza di violazioni delle disposizioni in materia di protezione dei dati personali, presenti, a conferma della rilevanza di detta tutela, sin dall'emanazione della Dir. 95/46/CE, dove all'art. 23, par. 2, veniva rigorosamente sancito – dovendosi esso interpetrare alla luce del considerando 55 che consentiva all'agente di provare *«l'esistenza di un errore della persona interessata o un caso di forza maggiore»* - che «(i)*l responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile*». A tale impostazione seguiva, sul piano nazionale, l'art. 15 del d.lgs. 196/2003, il quale – meno rigorosamente – sanciva che «*chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto*

al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 [*id est*: secondo quanto prescritto dalla stessa direttiva (cfr., *supra*, la nota n. 6)]», e, altresì, l'art. 82, par. 3, del Reg. 679/2016, a tenore del quale «*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile*», ponendo così all'interprete il delicato interrogativo se la nuova previsione avesse, o meno, modificato l'abrogato impianto normativo - a cui, nel presente scritto, si è tentato di fornire una risposta, a nostro parere appagante, alla luce dei principi e degli orientamenti giurisprudenziali nazionali esistenti sul punto, da ultimo confermati dalla Corte di Giustizia dell'Unione europea – dimostrando che siffatta responsabilità è di tipo oggettivo, seppure da classificare all'interno della categoria della c.d. "responsabilità oggettiva spuria", di elaborazione dottrinale, ma anche oggetto di avallo da parte della giurisprudenza costituzionale. Ne è testimonianza la circostanza, da un lato, che è consentita in capo al danneggiante una parziale inversione dell'onere probatorio (circostanza, questa, che ne permette l'inquadramento all'interno della famiglia delle "responsabilità oggettive"), dall'altro, che è comunque allo stesso consentita la possibilità di provare la propria estraneità all'evento lesivo, condizione, questa, che permette di collocare detto regime di imputazione al di fuori dell'area della "responsabilità oggettiva pura", la quale, come *supra* precisato, non prevede alcun margine di esenzione dall'imputazione dell'obbligazione risarcitoria.

La soluzione interpretativa suggerita è di accogliere una lettura dell'art. 82 del G.D.P.R. che consenta l'applicazione delle limitazioni probatorie già previste dall'art. 2050 c.c., sì da evitare, pur nel mutato regime normativo, soluzioni di continuità con il precedente dettato contenuto nell'art. 15 del Codice della Privacy, permettendo di ricondurre l'illecito trattamento di dati personali all'ipotesi di responsabilità oggettiva di cui all'art. 2050 c.c.. Pertanto, il danneggiato che lamenti la lesione dell'interesse non patrimoniale

può limitarsi a dimostrare l'esistenza del danno e del nesso di causalità rispetto al trattamento illecito, mentre spetta al danneggiante titolare del trattamento, eventualmente in solido col responsabile, dimostrare di aver adottato tutte le misure idonee per evitare il danno. Infatti, il titolare del trattamento, ai sensi del nuovo GDPR (art. 82, paragrafo 3) per non incorrere in responsabilità deve dimostrare che l'evento dannoso non gli è in alcun modo imputabile e non può limitarsi alla prova negativa di non aver violato le norme (e quindi di essersi conformato ai precetti), ma deve dar prova positiva di aver valutato autonomamente il rischio di impresa, purché tipico, cioè prevedibile, e attuato le misure organizzative e di sicurezza tali da eliminare o ridurre il rischio connesso alla sua attività. Ipotesi interpretativa, questa, a nostro parere sufficientemente appagante, per un verso, perché l'art. 82, par. 3, del Reg. 679/2016 si limita a precisare che «*3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile* (enfasi aggiunta)», per altro verso, perché dal tenore letterale dell'intero testo dell'art. 82 del G.D.P.R., non è dato cogliere alcuna precisazione, fortemente limitativa, di tenore analogo a quella presente nel considerando 55 dell'abrogata Dir. 95/46/CE (secondo cui l'imputabilità sarebbe stata esclusa solo allorquando fosse stata dimostrata «*l'esistenza di un errore della persona interessata o un caso di forza maggiore*»), con ciò lasciando all'elaborazione, dottrinale e giurisprudenziale, il compito di suggerire una lettura regolamentare in linea con le caratteristiche e i principi a cui è informato l'ordinamento nazionale.

Tale soluzione, oltre che nella giurisprudenza nazionale, ha trovato conforto nella giurisprudenza della Corte di Giustizia dell'Unione europea, la quale ha chiarito, per un verso, che la responsabilità risarcitoria di che trattasi può configurarsi, non già in presenza della mera violazione di disposizioni in materia di privacy, ma esclusivamente ove concorrano contestualmente (i) una violazione delle disposizioni del G.D.P.R., (ii) un evento lesivo e (iii) un nesso causale che

colleghi la violazione all'evento lesivo, spettando poi all'ordinamento giuridico di ciascuno Stato membro la previsione dei criteri che guidino il giudice nella concreta valutazione dell'entità del risarcimento, per altro verso, che la responsabilità risarcitoria per danno immateriale da parte del trasgressore si concretizza indipendentemente dalla gravità del danno medesimo, non rilevando l'eventuale tenuità del fatto.