amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Rivista scientifica trimestrale di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

Rivista di Ateneo dell'Università degli Studi di Roma "Foro Italico"

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei, Julián Espartero Casado

Direttore Responsabile
Gaetano Caputi

Redazione
Giuseppe Egidio Iacovino, Carlo Rizzo

FASCICOLO N. 1/2021

Estratto

Iscritta nel registro della stampa del Tribunale di Roma al n. 16/2009
ISSN 2036-7821

Comitato scientifico

Annamaria Angiuli, Antonio Barone, Vincenzo Caputi Jambrenghi, Enrico Carloni, Maria Cristina Cavallaro, Guido Clemente di San Luca, Andry Matilla Correa, Gianfranco D'Alessio, Ambrogio De Siano, Ruggiero Dipace, Luigi Ferrara, Pierpaolo Forte, Gianluca Gardini, Biagio Giliberti, Emanuele Isidori, Francesco Merloni, Giuseppe Palma, Alberto Palomar Olmeda, Attilio Parisi, Luca Raffaello Perfetti, Fabio Pigozzi, Alessandra Pioggia, Helene Puliat, Francesco Rota, Leonardo J. Sánchez-Mesa Martínez, Ramón Terol Gómez, Antonio Felice Uricchio.

Comitato editoriale

Jesús Avezuela Cárcel, Giuseppe Bettoni, Salvatore Bonfiglio, Vinicio Brigante, Giovanni Cocozza, Sergio Contessa, Mariaconcetta D'Arienzo, Manuel Delgado Iribarren, Giuseppe Doria, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Margherita Interlandi, Laura Letizia, Gaetano Natullo, Carmen Pérez González, Marcin Princ, Antonio Saporito, Giuliano Taglianetti, Salvatore Villani.

Coordinamento del Comitato editoriale

Valerio Sarcone.

ISSN 2036-7821

amministrativ@mente
Rivista scientifica trimestrale di diritto amministrativo
www.amministrativamente.com

UNIVERSITÀ DEGLI STUDI DI ROMA "FORO ITALICO"

Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva? *

di Filippo Lorè

(Docente a contratto Università degli studi di Bari "A. Moro" per l'insegnamento "Trattamento dei dati sensibili")

e Paolo Musacchio

(Data Protection Officer e avvocato esperto in diritto delle nuove tecnologie)

Sommario

1. Lo scenario normativo europeo in materia di protezione dei dati personali. - 2. Brevi cenni alla normativa in materia di cybersecurity. - 3. Le nuove sfide nella gestione della cybersecurity. - 4. Due figure fondamentali: il responsabile protezione dati e il responsabile per la transizione al digitale. - 5. Conclusioni.

Abstract

This article intends to analyze the recent European regulatory framework which, in the field of data security, focuses on the principle of accountability of the data controller, opening new perspectives, in the public and private sector, in terms of privacy governance. Therefore the analysis will concern, first of all, the Regulation (EU) 2016/679 and the related prescriptions, as well as the legislation on cybersecurity, object of attention by the Italian and European legislators, with the introduction of the NIS Directive, of the Cyber Act and the Perimetro nazionale di sicurezza cibernetica. The new challenges in these areas are decisive in the context of a society called upon to guarantee the free enjoyment of citizens fundamental rights and freedoms.

ISSN 2036-7821

1. Lo scenario normativo europeo in materia di protezione dei dati personali.

Il Regolamento (UE) 2016/679[1], in vigore dal 25 maggio 2018, si pone quali obiettivi principali la tutela dei diritti e delle libertà fondamentali delle persone fisiche, l'uniformità della normativa negli Stati membri, nonché la libera circolazione dei dati personali. Risulta opportuno ricostruire brevemente come si è arrivati a tale normativa, che, dando forma ad una politica europea comune dei dati personali, è un secondo punto di svolta nell'evoluzione del sistema multilivello di protezione dei dati, risultato di un approfondito confronto con sistemi diversi per cultura e tradizione giuridica, nei quali la tutela assicurata alle informazioni personali non raggiunge, o non sempre garantisce, un livello adeguato ai canoni europei[2]. In precedenza, il primo passo che aveva interrotto l'inerzia in materia di protezione dati, era stata l'adozione della Carta dei diritti fondamentali dell'Unione europea proclamata a Nizza nel 2000, che, sussumendo la dignità tra i valori «indivisibili e universali», aveva collocato la tutela dei dati personali nell'alveo dei diritti fondamentali della persona[3]. La Carta di Nizza, nel solo elencare e schematizzare i diritti che valgono in ambito UE, ha mostrato la sua portata innovatrice. Tra gli altri, quello per cui ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Ne deriva che il diritto alla protezione dei dati è, dunque, attribuito inderogabilmente, senza possibilità di prevedere limiti od esclusioni alla sua titolarità. Allo stesso tempo ne è individuata l'estensione quanto all'oggetto e al contenuto, riferiti alle condizioni che devono osservarsi affinché esso sia effettuato nel rispetto del principio di lealtà, di limitazione delle finalità, del consenso dell'interessato, oppure in presenza di un fondamento legittimo previsto dalla legge[4]. D'altronde, il diritto alla protezione dei dati personali, come riportato da Stefano Rodotà, «nell'età nuova del Web, della continua e massiccia produzione di profili, del *cloud computing*, dell'intelligenza artificiale, di sviluppi come quelli indicati dall'*automatic computing*», deve essere reinventato «non solo perché viene esplicitamente considerato come un autonomo diritto fondamentale, perché si presenta come strumento indispensabile per il libero sviluppo della personalità e per

* Benché il presente lavoro sia frutto della riflessione comune e della collaborazione dei due Autori, tuttavia, i paragrafi 2, 3 e 5 sono stati redatti da Filippo Lorè ed i paragrafi 1 e 4 sono stati redatti da Paolo Musacchio.

[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).

[2] R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, a cura di Cuffaro Vincenzo, D'Orazio Roberto, Ricciuto Vincenzo, Giappichelli Editore, 2019, p. 61 ss.

[3] R. D'ORAZIO, *Ibidem.* In proposito v. L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO – C. COLAPIETRO, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017

[4] R. D'ORAZIO, *Ibidem*

ISSN 2036-7821

definire l'insieme delle relazioni sociali»[5]. Ai fini della nostra trattazione, giova premettere che una delle grandi innovazioni del Reg. UE 2016/679 è il suo ambito di applicazione. Considerato che la Direttiva 95/46/CE proponeva un approccio statico alla tutela e al trasferimento dei dati, incentrato sulla visione proprietaria del dato, il legislatore europeo del 2016 ha voluto, differentemente, introdurre due criteri per la definizione dell'ambito di applicazione del Reg. UE 2016/679, al fine di estendere l'efficacia spaziale: il criterio di stabilimento, per cui il luogo del trattamento è irrilevante, e il criterio del *target*, che impone di prendere in considerazione l'ubicazione degli interessati. La vigenza della disciplina europea in materia di protezione dei dati riguarda, dunque, il titolare del trattamento o il responsabile del trattamento, anche non stabiliti nell'Unione, le cui attività di trattamento riguardano, tuttavia, l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione[6]. Ed è proprio sui soggetti attivi che, direttamente o indirettamente, operano sulle informazioni personali, che il Regolamento ha inciso in maniera significativa, poiché i relativi ruoli devono essere reinterpretati, adottando l'approccio sostanzialistico di *substance over form*[7]. Il legislatore europeo, a tal riguardo, delinea figure non riconducibili alla classica dicotomia "diritto reale-rapporto obbligatorio", configurando una trama normativa di matrice pubblicistica[8], alla cui sommità è posta l'Autorità garante per la protezione dei dati personali. Stabilito che il fine ultimo del Regolamento è la protezione dei diritti e delle libertà delle persone fisiche cui i dati personali si riferiscono, è innegabile la centralità della figura del titolare. Ai sensi dell'art. 2-*quaterdecies* del Codice novellato, infatti, nell'ambito della sua organizzazione, il titolare può individuare dei soggetti autorizzati[9], mediante la produzione di un atto formale che contenga le istruzioni e le modalità attuative delle attività rilevanti, mediante espresso rinvio ai principi del trattamento. Per i soggetti ai quali il titolare abbia invece deciso di esternalizzare alcune delle sue attività, se queste prevedono un trattamento di dati personali, è, altresì, necessaria la formalizzazione dei rapporti mediante una nomina a

[5] S. RODOTÀ, *Il diritto di avere diritti*, Editori Laterza, 2012, p. 319 e ss.

[6] V. anche COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (EDPB), *Linee-guida 3/2018 sull'ambito di applicazione territoriale del REG. UE 2016/679 (articolo 3) - version adopted after public consultation*, 12 novembre 2019, in https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_it

[7] G. CONTI, *La protezione dei dati personali per titolari e responsabili del trattamento*, Maggioli Editore, 2019, p. 51

[8] N. BRUTTI, *Le figure soggettive delineate dal GDPR, la novità del Data Protection Officer*, in *Privacy digitale*, a cura di Emilio Tosi, Giuffré, 2019, p. 119

[9] Art. 2-Quaterdecies, DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali", come modificato dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

responsabile del trattamento ("*Data processor*"), figura che, nella definizione del Reg. UE 2016/679 è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi del citato Regolamento. Tale *Data Processing Agreement* deve contenere tassativamente gli obblighi cui il responsabile del trattamento (che nel nuovo impianto normativo è necessariamente esterno all'organizzazione del titolare) è chiamato a rispondere, vale a dire garantire che il proprio personale abbia un adeguato obbligo legale di riservatezza, rispettare le condizioni per ricorrere a un sub-responsabile del trattamento, assistere il titolare nel rispetto degli obblighi di sicurezza e nello svolgimento della valutazione di impatto *privacy*, avvertire, senza ingiustificato ritardo, il *Data Controller* al ricorrere degli eventi di *data breach*, cancellare e restituire i dati al termine del trattamento, in un formato adeguato e secondo modalità adeguate al progresso tecnologico. Risulta opportuno segnalare, per i profili richiamati, anche il Considerando 79[10], Reg. UE 2016/679, laddove chiarisce che la protezione dei diritti e delle libertà degli interessati, così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, esige una chiara ripartizione delle responsabilità, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento, o quando l'operazione di trattamento venga eseguita per conto del titolare del trattamento. Purtuttavia, con riferimento all'aspetto sostanziale, che ben si sposa con l'*accountability* richiesta dalla normativa rilevante in materia di protezione dati, non è sempre cristallina la categorizzazione tra la situazione di contitolarità e il rapporto di "soggezione", tipico della subordinazione del responsabile del trattamento nei confronti del titolare. L'art. 26, Reg. UE 2016/679, in tal senso, dispone che, qualora due o più titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento, questi sono da considerare quali contitolari del trattamento, con il conseguente onere di formalizzare, in modo trasparente e mediante un accordo interno, le rispettive responsabilità in merito all'osservanza delle prescrizioni impartite dal legislatore europeo in materia di protezione dati, con particolare riguardo all'esercizio dei diritti degli interessati, a disposizione dei quali può essere designato, dai contitolari, un punto di contatto, quale figura di garanzia. Ad ogni modo, autorevole dottrina ha ulteriormente affermato che, qualora il potere decisionale relativo alle modalità di svolgimento del trattamento sia ripartito tra più soggetti, ed a ciascuno di essi spetti, per la parte di competenza, il c.d. *risk assessment* e la determinazione delle conseguenti misure tecniche ed organizzative da adottare,

[10] Giova ricordare, come affermato dalla Corte di Giustizia dell'UE, che il Considerando di un Regolamento, pur non essendo giuridicamente vincolante, «può […] consentire di chiarire l'interpretazione di una *regula juris*» (CGUE, sentenza 13 luglio 1989, causa C-215/88, Casa Fleischhandel / BALM, punto 31).

ISSN 2036-7821

costoro devono essere qualificati come contitolari[11]. Rilevantissima innovazione del Reg. UE 2016/679, prevista all'art. 37, è l'introduzione della figura del responsabile protezione dati (o *data protection officer*), alla cui trattazione si rinvia[12]. La panoramica dei soggetti attivi contempla, altresì, la figura dell'Amministratore di sistema, non esplicitamente richiamata nel Regolamento. L'ambito di responsabilità di tale soggetto sulle operazioni di trattamento dati personali riveste un ruolo fondamentale, in particolar modo per le attività legate alla sicurezza delle banche dati e alla corretta gestione delle reti telematiche. Allo stesso, invero, è demandato l'obbligo di vigilare sul corretto utilizzo dei sistemi informatici, la facoltà di abilitare gli utenti all'accesso alle banche dati, l'attribuzione agli utenti dei profili di autorizzazione, determinati sulle specifiche attività poste in essere dagli autorizzati, che consentono la visibilità dei dati, anche di natura personale, in rapporto ai compiti effettivamente svolti[13]. L'amministratore di sistema, sostanzialmente, è chiamato a mettere in atto misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza adeguato al rischio, secondo indicazione che il Garante, nel 2008,[14] aveva contribuito a rideterminare. In tale Provvedimento, l'Autorità, sulla base delle attività ispettive pianificate nel corso degli anni, ha stabilito l'obbligo per il titolare di designare individualmente i singoli amministratori di sistema, a mezzo di un atto preordinato ad elencare, analiticamente, gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. In aggiunta, preme ricordare che il legislatore europeo ha sancito il principio cardine della «liceità del trattamento» dei dati personali e, dunque, elencato, all'art. 6 del Regolamento, le basi giuridiche su cui può essere fondato il trattamento, ossia il consenso dell'interessato, l'esecuzione di un contratto (o misure precontrattuali) di cui l'interessato è parte, l'adempimento di un obbligo legale del titolare del trattamento, la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, l'attuazione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e il perseguimento del legittimo interesse del titolare del trattamento o di terzi, sempreché, su quest'ultima base giuridica, non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati, in particolare se l'interessato è un minore. L'utilizzo della base giuridica del legittimo interesse si attaglia come

[11] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali, il Regolamento europeo 2016/679*, Giappichelli editore, 2016, p. 55-57

[12] *Infra*, paragrafo 4

[13] F. MODAFFERI, Lezioni di diritto alla protezione dei dati personali, Lulu Editore, 2015, p. 213-214

[14] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento Generale 27 novembre 2008, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema con l'intento di promuovere presso Titolari e pubblico la consapevolezza della delicatezza del ruolo di amministratore di Sistema (modificato il 25 giugno 2009). Con il DECRETO LEGISLATIVO 10 agosto 2018, n. 101, che ha modificato il DECRETO LEGISLATIVO 30 giugno 2003, n.196, i provvedimenti del Garante antecedenti al 25 maggio 2018 restano in vigore ove compatibili con il REG. UE 2016/679 e con il nuovo Codice *Privacy*.

ISSN 2036-7821

un'operazione delicata, poiché lo stesso è sotteso ad una situazione giuridica definita, all'esito di una valutazione in ordine al bilanciamento degli interessi coinvolti a cura del titolare del trattamento, chiamato dalla normativa richiamata a valutare autonomamente, nell'ambito del principio di *accountability*, la sussistenza di un legittimo interesse suo, o di terzi, a condizione che non prevalgano i diritti degli interessati[15]. In tal senso, secondo una lettura estensiva del Considerando 47, Reg. UE 2016/679, potrebbe sussistere il legittimo interesse in presenza di una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento. La stessa base giuridica, come affermato più volte nelle interlocuzioni formali del Garante, non può, tuttavia, essere invocata da alcun titolare incardinato nel settore pubblico o privato, per effettuare operazioni di trattamento sulle categorie particolari di dati, o dalle Autorità pubbliche, nell'assolvimento dei propri compiti istituzionali[16]. Risulta opportuno, alla luce di quanto detto, soffermarsi sulle categorie di dati personali poiché tali dati possono assumere connotazioni diverse. L'art. 9, Reg. UE 2016/679, conduce ad un generico divieto di trattamento dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, informazioni relative alla salute, alla vita sessuale o all'orientamento sessuale della persona. Tali dati personali, definiti "particolari", ricalcano in gran parte la categoria dei dati definiti "sensibili" nella vecchia formulazione del Codice. Il trattamento di tali categorie di dati, constando di informazioni relative ad aspetti delicati ed intimi della vita delle persone fisiche, presenta forti criticità, poiché un trattamento illecito degli stessi o una violazione dei dati trattati espone gli interessati a serie conseguenze in ordine al libero godimento delle libertà fondamentali. Per tale ragione, il legislatore europeo in materia di protezione dati pone un argine al trattamento delle categorie particolari di dati, fotografando un generale divieto, che viene temperato da alcune significative eccezioni previste dall'art. 9, comma 2, Reg. UE 2016/679, quali, a titolo esemplificativo, i trattamenti basati sul consenso dell'interessato, sull'adempimento di obblighi legali cui è soggetto il titolare, sull'esecuzione di un compito di interesse pubblico rilevante, ai sensi dell'art. 2-*sexies*, Codice novellato, sull'esigenza di tutelare un interesse vitale, sull'essenzialità di accertare, esercitare o difendere un diritto in sede giudiziaria, sull'istanza di archiviazione nel pubblico interesse, di ricerca scientifica, storica o a fini statistici, e sull'instaurazione del rapporto di lavoro

[15] L. CALIFANO, *Spunti problematici sul trattamento dei dati personali raccolti tramite droni*, in *Cultura giuridica e diritto vivente*, Vol. 7, 2020, p. 4

[16] D. KORFF, M. GEORGES, CON IL CONTRIBUTO DEL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI PERSONALI & DEI PARTNER DEL PROGETTO, *Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea*, versione approvata dalla Commissione, luglio 2019, p. 199

ISSN 2036-7821

tra titolare e interessato[17]. È di tutta evidenza come il legislatore europeo in materia di protezione dati, da una attenta analisi dell'articolo 9, Reg. UE 2016/679, preveda basi giuridiche specifiche su cui si fondare il trattamento dei dati "particolari", rispetto a quelle generali riportate nell'art. 6 della disciplina rilevante in materia. Per ciò che attiene, in ultimo, alla categoria dei dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza, il trattamento di tali dati deve avvenire soltanto sotto il controllo dell'autorità pubblica o se lo stesso è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati[18], disposizione quasi interamente richiamata nell'art. 2-*octies*, comma 1, Codice novellato, laddove consente, fatto salvo quanto previsto dal d.lgs. 18 maggio 2018, n. 51[19], il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza, solo in presenza di un'apposita norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati. Ne deriva che, a titolo esemplificativo, è lecito il trattamento di tali tipi di dati personali al configurarsi di situazioni ben delineate. Si pensi, nell'ambito pubblico, alle disposizioni in materia di comunicazioni e informazioni antimafia, o anche alle disposizioni vigenti in materia di appalti, considerato che spesso il trattamento di dati relativi a condanne penali si rende necessario nell'ambito delle procedure di appalti pubblici, servizi e forniture, ovvero per poter sottoscrivere contratti di lavoro. Analoghe valutazioni valgono anche per le norme della legge 30 novembre 2017, n. 179, in materia di lotta ai fenomeni corruttivi (*whistleblowing*), nonché per quelle contenute nelle leggi di

[17] G. CONTI, *La protezione dei dati personali per titolari e responsabili del trattamento*, Maggioli Editore, 2019, p. 42 ss.

[18] Art. 10 REG. UE 2016/679. In precedenza, l'articolo 27 del Codice *Privacy* consentiva il trattamento dei dati giudiziari da parte di privati o di enti pubblici economici soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specificasse le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Con l'autorizzazione generale n. 7 del 15 dicembre 2016, il Garante aveva indicato una serie di ambiti nei quali, rispettando specifiche prescrizioni ivi contenute e fermi restando i principi generali della disciplina tra cui quello della minimizzazione del trattamento dei dati personali, il trattamento dei dati giudiziari era legittimo (rapporti di lavoro; attività di associazioni e fondazioni; attività dei liberi professionisti; imprese bancarie e assicuratrici; attività di investigazione privata; produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto; accertamento dell'idoneità morale di coloro che intendono partecipare a gare di appalto; adempimento degli obblighi previsti dalle disposizioni in materia di comunicazione e certificazioni antimafia; attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese). Il garante è intervenuto, con il Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101 - 5 giugno 2019, sancendo l'incompatibilità con il REG. UE 2016/679 dell'autorizzazione generale n. 7/2016, rendendola di fatto inoperante, tuttavia essa resta un riferimento importante, in attesa dell'intervento del legislatore (e del Ministro della Giustizia, ai sensi del comma 2 dell'art. 2-octies del Codice novellato).

[19] DECRETO LEGISLATIVO 18 maggio 2018, n. 51, Attuazione della 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.

ISSN 2036-7821

contrasto al terrorismo (legge 15 dicembre 2001, n. 438 e legge 17 aprile 2015, n. 43). Appare opportuno, a questo punto, rivisitare sinteticamente anche i principi generali applicabili in ogni fase del trattamento dei dati personali. Il Regolamento UE 2016/679, infatti, all'art. 5, elenca tali principi, ricalcando, in buona parte, la disposizione di cui all'art.11, della vecchia formulazione del d.lgs. n. 196/2003. Oltre ai principi, richiamati in precedenza, della «liceità del trattamento» dei dati personali, e quello per cui i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, il legislatore europeo impone, in primo luogo, che i dati siano esatti ed aggiornati. Con riferimento al rapporto tra titolare e interessato, il legislatore europeo ha dedicato un intero Capo (il III) del Regolamento ai diritti dell'interessato. Il trattamento dei dati personali deve essere corretto e trasparente, derivandone che il più importante diritto riconosciuto all'interessato è quello del diritto all'informazione in ordine alla raccolta dei dati personali che lo riguardano. Il legislatore europeo dispone, *apertis verbis*, che l'informativa debba essere rilasciata in forma concisa, trasparente, intelligibile per l'interessato, facilmente accessibile, mediante un linguaggio chiaro e semplice, e secondo formule di garanzia per i soggetti di minore età. Completa la Sezione 2 del Capo III un altro diritto «informativo», vale a dire il diritto di accesso che consente al'interessato di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle relative informazioni ovvero le finalità del trattamento, le categorie di dati trattati, i destinatari, il periodo di conservazione, i diritti esercitabili dall'interessato, l'esistenza di un processo decisionale automatizzato, compresa la profilazione. La Sezione 3 del Capo III del Regolamento è dedicata invece ai diritti di «Rettifica e cancellazione» che configurano la possibilità di ottenere la rettifica dei dati, la cancellazione, la limitazione del trattamento, la notifica del titolare in caso di rettifica, cancellazione dei dati personali o limitazione del trattamento, e la portabilità dei dati. Evidente risulta la spinta del legislatore europeo in materia di protezione dati in ordine all'autodeterminazione dell'interessato, intesa quale piena realizzazione della sua sfera privata mediante il controllo dei flussi di informazioni che lo riguardano. Al modello statico, fondato sul diritto di difendersi da interferenze con la propria sfera privata, si è andata via via affiancando una forma di tutela dinamica, che assicura un potere di reazione ed una serie ampia di garanzie di tipo organizzativo e procedurale[20], consacrata nella Direttiva "Madre" del 1995 e recepita nella legge 31 dicembre 1996, n. 675[21]. L'inadeguatezza della prospettiva civilistica nostrana che operava *ex post*, cioè soltanto dopo che la lesione si era manifestata ha, difatti, indotto

[20] G. MARINI, *Diritto alla privacy*, in A. BARBA, S. PAGLIANTINI, *Commentario del Codice civile diretto da Enrico Gabrielli*, Vol. III: Delle Persone - Leggi collegate, UTET, 2013, p. 222 ss.

[21] Legge 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"

ISSN 2036-7821

il legislatore nazionale a promuovere una tutela *ex ante* capace di prevenire possibili occasioni di danno e pregiudizio, attraverso una serie di regole riguardanti le modalità di trattamento dei dati e i poteri di intervento indispensabili per seguire i dati nella loro circolazione[22]. Il perimetro della portata del diritto di accesso era stato esteso dal Codice *privacy* del 2003 (art. 7, comma 2, lettere b e c, norma abrogata nel 2018), anche alle «modalità del trattamento» e alla «logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici» con la conseguente configurazione di una situazione strumentale poiché permetteva l'esercizio di altri diritti, quali l'aggiornamento, la rettifica, l'integrazione, la trasformazione in forma anonima ed il blocco dei dati, che consentivano di non perdere il controllo della propria identità in relazione alle attività svolte da altri soggetti[23]. Come osservato in dottrina, il legislatore aveva inteso affidare al Codice l'operatività di una strategia di "ricomposizione" del soggetto dinanzi alla possibile frammentazione della sua identità in una serie di dati (dimensione sincronica) o dalla sua dispersione nel tempo (dimensione diacronica), stante la possibilità che le fisiologiche visioni parziali dell'identità che derivano dalle diverse raccolte di dati, moltiplichino le possibilità di deformazione, controllo tecnologico e classificazione degli individui ("identità sincronica")[24]. È opportuno fare cenno anche al (nuovo) diritto alla portabilità del dato, segnalandosi, però, che sono portabili le sole informazioni personali trattate sulla base del consenso, espresso e libero, o sulla base di un contratto stipulato, e limitatamente ai dati che siano stati "forniti" dall'interessato al titolare. Per tutti i diritti dell'interessato, il termine per la risposta del titolare del trattamento è misurato nel termine di un mese, estendibile fino a tre mesi in casi di particolare complessità, al decorrere del quale il titolare deve comunque produrre un riscontro all'interessato, anche in caso di diniego. Con riferimento, invece, al diritto all'oblio, esso è una particolare declinazione del diritto dell'interessato alla cancellazione del dato personale trattato in violazione della legge, per gli ovvi problemi che emergono qualora l'interessato esiga di "essere dimenticato" nell'ambito dei servizi *online*. Sovente, per determinare l'esistenza del diritto all'oblio, si valuta la sussistenza di un interesse pubblico alla conoscenza dei fatti. Tra i tanti arresti giurisprudenziali intervenuti sull'argomento, molti di essi hanno precisato che finanche la riemersione di un fatto molto lontano nel tempo, che all'epoca rivestiva un sicuro interesse

[22] S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy*, in *Europa e diritto privato*, n. 1, 2004, p. 2

[23] G. MARINI, *Diritto alla privacy*, in A. BARBA, S. PAGLIANTINI, *Commentario del Codice civile diretto da Enrico Gabrielli*, Vol. III: Delle Persone - Leggi collegate, UTET, 2013, p. 222 ss.; Cfr. anche S. RODOTÀ, *Privacy e costruzione della sfera privata*, in Tecnologie e diritti, Bologna, 1995; S. RODOTÀ, *Intervista su privacy e libertà*, a cura di P. Conti, Roma-Bari, 2005; S. RODOTÀ, *Tra diritto e società. Informazioni genetiche e tecniche di tutela*, Riv. critica dir. priv., 2000, 571; S. RODOTÀ, La vita e le regole. Tra diritto e non diritto, Milano, IV ed., 2007.

[24] S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, Riv. critica dir. priv., 1997, p. 583.

ISSN 2036-7821

pubblico, non si traduce, *ipso facto*, nella permanenza dell'interesse anche nel momento attuale[25]. La giurisprudenza europea ha peraltro evidenziato la necessità della prevalenza del diritto alla cancellazione dei dati a fronte dell'interesse pubblico all'informazione non giustificato da particolari ragioni obiettive[26]. Il diritto all'oblio costituisce dunque un interesse tutelato dall'ordinamento e avente come fonte la giurisprudenza cd. normativa, che lo ha identificato nella situazione soggettiva di chi, in contrapposizione al diritto di cronaca (e di critica), ha interesse a che non siano pubblicizzate, mediante l'attività di informazione, vicende che lo riguardano ma che risultano risalenti nel tempo e che già hanno costituito oggetto di attività di informazione[27]. Tale interesse, connesso alla tutela dell'identità personale e della riservatezza, è fondato sulla non attualità dell'interesse pubblico a conoscere determinate vicende[28]. Con l'applicabilità del Reg. UE 2016/679 (e con la conseguente abrogazione dell'art. 11 del Codice *Privacy* operata dal legislatore del 2018) il diritto all'oblio ha una disciplina organica, stanti gli articoli 17, 19 e 21 del Reg. UE 2016/679, tuttavia restano aperte, per il diritto all'oblio, rilevanti questioni alle quali il legislatore europeo non ha dato soluzione[29], in special modo nell'ambiente *online*. Pertanto, le informazioni personali devono essere utilizzate rispettando il presupposto della minimizzazione. La panoramica sui diritti degli interessati può terminare con la descrizione della Sezione 4 del Capo III del Regolamento, dedicata al diritto di opposizione dell'interessato ai trattamenti di dati personali che lo riguardano, compresi i processi decisionali automatizzati e le profilazioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. A tenore dell'art. 22, Reg. UE 2016/679, invece, sussiste il diritto dell'interessato a non subire decisioni basate unicamente su trattamenti automatizzati, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida, in modo analogo, significativamente sulla sua persona, norma da raccordare all'art. 15, par. 1, lettera h, laddove stabilisce che l'interessato ha diritto a conoscere l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. La dottrina è concorde

[25] *Ex multis*, Cass. Civ., 26 giugno 2013, n. 16111, in Foro.it

[26] V. CGUE, Causa C – 131/12, *Google Spain e Inc. vs. Agencia Espanola de Proteccion de Datos e Mario Costeja Gonzalez*, 13 maggio 2014)

[27] S. RUSCICA, P. MONTONE, N. TILLI, *Il diritto all'oblio dopo il nuovo regolamento europeo sulla privacy*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali*, 2017, p. 110

[28] S. RUSCICA, P. MONTONE, N. TILLI, *Ibidem*, p. 111

[29] V. in tal senso F. DI CIOMMO, *Il diritto all'oblio nel Regolamento (UE) 2016/679. Ovvero, di un "tratto di penna del legislatore" che non manda al macero alcunché*, in Il Corriere Giuridico, 2018

nell'affermare che il soggetto destinatario di una decisione basata «unicamente sul trattamento automatizzato» nell'accezione di cui all'art. 22, par. 1, abbia diritto ad essere informato, prima del trattamento, in relazione al se una decisione automatizzata sarà assunta nei confronti. L'interessato potrà poi ottenere conferma del fatto che una decisione automatizzata sia stata effettivamente assunta esercitando il diritto accesso di cui all'art. 15. Il contenuto dell'art. 15 è infatti analogo a quella degli artt. 12 e 13, anche se cambia la struttura, essendo il diritto d'accesso a trasparenza reattiva e non proattiva, poiché il titolare del trattamento dovrà fornire le informazioni solo a fronte di una richiesta dell'interessato. Parte della dottrina ritiene che, anche in mancanza di specifica elaborazione legislativa, esista un diritto di avere una spiegazione in relazione al processo decisionale automatizzato, ossia ottenere informazioni generali sulla funzionalità dell'algoritmo e sulle conseguenze previste del trattamento automatizzato[30]. La stessa dottrina si è interrogata in maniera approfondita anche sull'esistenza di un "diritto alla spiegazione" dell'algoritmo su cui si basa una profilazione, stante la lettura del Considerando 71 del Regolamento, laddove ricomprende, tra le "garanzie adeguate" dell'interessato cui dovrebbe essere subordinato un trattamento automatizzato, il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare tale decisione. Più in particolare, ci si è chiesti cosa significhi (e cosa sia necessario per) spiegare la decisione di un algoritmo. Il *machine learning*, in particolare negli algoritmi di apprendimento automatico supervisionato, si basa sullo scoprire associazioni e correlazioni affidabili, senza preoccuparsi più di tanto delle cause e delle spiegazioni che vanno oltre gli scopi puramente statistici. Orbene, l'uso di decisioni algoritmiche ha portato la dottrina a mettere in guardia dall'implementazione di sistemi che possono rappresentare una Società basata su una "scatola nera", in mancanza di una trasparenza del processo decisionale algoritmico[31]. Tornando alla rassegna dei principi del Regolamento, con riferimento al predetto principio di minimizzazione, esso impone che siano oggetto di trattamento soltanto i dati «adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati»[32]. Le categorie di dati scelte per il trattamento devono rispondere all'obiettivo generale dichiarato dal titolare del trattamento, il

[30] B. GOODMAN, S. FLAXMAN, *European Union Regulations on algoritmic decision making and a "right to Explanation"*, Association for the Advancement of Artificial Intelligence, 2016.

[31] B. GOODMAN, S. FLAXMAN, *Ibidem*. Cfr. anche G.GAUDIO, *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo*, in *Labour&Law Issues*, vol. 6, no. 2, 2020; S. WACHTER, B.MITTELSTADT, L. FLORIDI, *Why a right to explanation of automated decision-making does not exist in the general data protection Regulation*, in *International Data Privacy Law*, 2017, vol. 7, no. 2; T. W. KIM, B. R. ROUTLEDGE, *Informational Privacy, A right to explanation, and interpretable AI*, in *IEEE Symposium on Privacy-Aware Computing*, 2018

[32] V. Convenzione n. 108 modernizzata, articolo 5, paragrafo 4, lettera c)

ISSN 2036-7821

quale, a sua volta, dovrebbe limitare rigorosamente la raccolta dei dati indispensabili allo scopo specifico perseguito[33]. L'articolo 5, paragrafo 1, della Convenzione n. 108 modernizzata, contiene, dunque, la previsione del requisito di proporzionalità delle attività di trattamento dei dati personali in relazione allo scopo legittimo perseguito, che è rappresentato dalla sussistenza del giusto equilibrio fra tutti gli interessi in gioco e per tutte le fasi del trattamento. Questo significa che i «dati personali che sarebbero adeguati e pertinenti, ma implicherebbero un'ingerenza sproporzionata nei diritti e nelle libertà fondamentali in gioco, devono essere considerati eccessivi»[34]. In sostanza, il principio in commento ha efficacia trasversale e implica una riduzione al minimo del numero dei dati, del tipo dei trattamenti, dei soggetti che a vario titolo possono avere contezza dei dati e del periodo di conservazione. Risulta necessario, in tale scenario, ridurre al minimo le operazioni di trattamento sui dati personali o, in alternativa, progettare misure tecniche ed organizzative utili a ridurre l'identificazione, anche indiretta, dell'interessato, offrendo una soluzione rispettosa della vita privata, mediante, ad esempio, la tecnica della pseudonimizzazione[35]. Secondo una stretta correlazione, altro principio degno di menzione è l'*accountability* del titolare del trattamento, enunciata agli artt. 5 e 24, Reg. UE 2016/679. Tale principio, che si sostanzia nella responsabilizzazione del titolare del trattamento, affinché quest'ultimo "sia in grado" (*to be able to*) di "rendicontare" (*account*) il rispetto dei principi della normativa rilevante in materia, impone al titolare l'adozione di misure tecniche e organizzative adeguate. Diretta derivazione dell'*accountability* del titolare è la protezione dei dati fin dalla progettazione (by design) e la protezione per impostazione predefinita (by default), principi enunciati nell'art. 25 della legislazione europea in materia di protezione dati. Affinché possa operare al meglio, infatti, la protezione dei dati deve essere integrata nell'intero ciclo di vita di una tecnologia, di un servizio o di un processo, sin dalla relativa progettazione[36]. In ultimo, perno centrale dell'impianto normativo del Regolamento 2016/679 è il principio di sicurezza del trattamento, enucleato nell'art. 32, laddove stabilisce che il titolare e il responsabile del trattamento «mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso

[33] FRA – AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, CORTE EUROPEA DEI DIRITTI DELL'UOMO (CONSIGLIO D'EUROPA), GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Manuale del diritto europeo in materia di protezione dei dati*, 2018, p. 142

[34] Relazione esplicativa della Convenzione n. 108 modernizzata, punto 52.

[35] N. BERNARDI (a cura di), *Privacy. Protezione e trattamento dei dati*, Wolters Kluwer, 2020, p. 82

[36] E. LUCCHINI GUASTALLA, *Privacy e data protection: principi generali*, in *Privacy digitale*, a cura di Emilio Tosi, Giuffré, 2019, p. 86

ISSN 2036-7821

dei dati personali in caso di incidente fisico o tecnico; una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento». Questa elencazione non è chiaramente esaustiva, poiché si rende necessario valutare il caso concreto, in base al livello di rischio individuato. Va segnalato che, con l'abrogazione dell'art. 33 e dell'Allegato B del Codice *Privacy*, intervenuta ad opera del d.lgs. 10 agosto 2018, n. 101, oggi non esistono più nel nostro ordinamento le "Misure minime di sicurezza" contenute nel richiamato Allegato (quali autenticazione, autorizzazioni, liceità dei trattamenti, backup, Documento Programmatico sulla Sicurezza (DPS), cifratura)[37]. In tale contesto, può rappresentare una minaccia per i diritti delle persone fisiche, una violazione dei dati personali ovvero, ai sensi dell'4, n. 12, Reg. UE 2016/679, la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. Le misure di sicurezza tecniche e organizzative, che devono essere progettate alla luce della prassi consolidata, devono garantire, infatti, un livello di sicurezza adeguato al rischio (art. 32, Reg. UE 2016/679). Invero, le violazioni dei dati possono interessare la riservatezza, qualora si verifichi una divulgazione o un accesso a dati personali non autorizzato o accidentale, l'integrità, nel momento in cui si determini un'alterazione di dati personali non autorizzata o accidentale, e la disponibilità, ove si accerti la perdita, l'inaccessibilità, o la distruzione, accidentali o non autorizzate, di informazioni personali. Quanto agli obblighi in capo al titolare del trattamento, in caso di violazione dei dati, egli è tenuto, tranne che nel caso in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, a notificare l'evento all'Autorità di controllo nazionale senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza[38]. Ancora, nell'ipotesi in cui dalla violazione dei dati personali possa derivare un forte pericolo per i diritti e le libertà fondamentali degli interessati, questi ultimi devono essere informati dal titolare, senza ingiustificato ritardo, al fine di consentire loro di avviare le azioni necessarie a limitare le conseguenze derivanti dalla predetta violazione.

2. La normativa in materia di cybersecurity.

Il quadro normativo in esame è ulteriormente delineato dalle disposizioni del legislatore europeo e nazionale in materia di sicurezza informatica, ramo che si

[37] V. anche art. 132-ter, DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali", come modificato dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101

[38] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento sulla notifica delle violazioni dei dati personali (data breach), 30 luglio 2019, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9126951*

ISSN 2036-7821

occupa dell'analisi delle minacce, della vulnerabilità e del rischio associato agli *asset* informatici, al fine di proteggere gli stessi da attacchi che potrebbero provocare danni rilevantissimi[39]. Il termine è spesso sostituito con il neologismo "*cybersecurity*", con cui si vuole intendere un approccio mirato ad enfatizzare non tanto le misure di prevenzione di accadimento delle minacce, quanto quelle di protezione, che tendono a mitigare la gravità del danno realizzato al verificarsi di una minaccia[40]. In tale direzione, fondamentale, in ambito UE, è stata l'adozione, nel 2016, della Direttiva NIS[41] (*Network and Information Security*), attuata in Italia con il d.lgs. 18 maggio 2018, n.65, che funge da "armonizzazione minima", con l'eccezione dei fornitori di servizi digitali, per i quali è misura di "armonizzazione massima"[42]. Ne deriva che tale normativa ha rappresentato la prima legislazione "orizzontale" preordinata ad affrontare le nuove sfide della *cybersecurity* e che vede, tra i suoi scopi, il miglioramento e il potenziamento delle capacità degli Stati membri, il rafforzamento della cooperazione, e, in particolar modo, la promozione di una cultura di gestione del rischio e di segnalazione degli incidenti tra gli operatori economici di servizi essenziali (OES o OSE) e i fornitori di servizi digitali (DSP), i quali sono tenuti all'adozione di misure tecniche ed organizzative adeguate, preordinate alla prevenzione degli incidenti informatici, da notificare al *Computer Security Incident Response Team* (CSIRT) e alle Autorità competenti NIS, autorizzate, altresì, ad irrogare sanzioni amministrative. L'aumento dei livelli di *cybersecurity* e dell'armonizzazione dei medesimi nell'Unione passa per il ruolo fondamentale di coordinamento dell'Agenzia dell'Unione europea per la *cybersecurity* (ENISA)[43]. Proprio con il precipuo scopo di delineare la cornice normativa, il 27 giugno 2019, è entrato in vigore una prima parte del Regolamento (UE) 2019/881[44], anche detto *Cybersecurity Act* o *CyberAct*, che ha rafforzato il ruolo dell'ENISA e definito un quadro UE per l'introduzione di sistemi europei di certificazione della *cybersecurity* dei prodotti, dei servizi e dei processi. Il citato Regolamento ha lo scopo di rendere sicuro il mercato unico digitale, di favorire un elevato livello di *cybersecurity*, di *cyber* resilienza e di fiducia all'interno dell'Unione. Con riguardo al ruolo affidato ad ENISA, invece, il *CyberAct* ha previsto nuove competenze, per prima quella legata al conseguimento di

[39] M. MAGLIO, *Cybersecurity e dati personali*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali*, 2017, p. 719

[40] M. MAGLIO, *Ibidem*

[41] 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

[42] F. LORÈ, *La sicurezza dei dati personali: misure e strategie alla luce delle recenti novità normative in materia di cyber security*, in Ratio Juris, Settembre 2019

[43] F. LORÈ, *Ibidem*

[44] REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»)

ISSN 2036-7821

un elevato livello comune di *cybersecurity* nell'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nelle azioni di miglioramento delle *best practices*. In tale contesto, su base nazionale, non può trascurarsi il Piano Triennale per l'Informatica nella pubblica amministrazione, redatto da AgID e approvato dal Presidente del Consiglio, che funge, per i pubblici Uffici, da supporto nella definizione del processo di trasformazione digitale e di sviluppo dei sistemi informativi, in attuazione del d.lgs. 7 marzo 2005, n. 82. Il Piano fissa i principi fondamentali, le regole di usabilità e interoperabilità, la logica di classificazione delle spese ICT, nell'ottica di una razionalizzazione di spesa e di miglioramento dei servizi offerti a cittadini e imprese. Più in particolare, il Piano Triennale 2020-2022[45], naturale evoluzione della versione precedente, punta principalmente allo sviluppo della digitalizzazione delle amministrazioni pubbliche, alla sostenibilità ambientale e alla maggiore diffusione delle nuove tecnologie digitali nel settore privato, mediante incentivi alla standardizzazione, innovazione e sperimentazione nell'ambito dei servizi pubblici, con particolare attenzione alla misurazione dei risultati e alla qualità dei dati. In tale contesto, principio assolutamente rilevante è quello della "sicurezza e *privacy by design*". Orbene, i servizi digitali devono essere progettati ed erogati in modo sicuro, favorendo l'adozione di meccanismi di tutela dei dati personali. Strettamente correlato a quanto riportato, infine, è il "Perimetro di sicurezza nazionale cibernetica"[46], introdotto nel nostro ordinamento dalla legge 18 novembre 2019, n. 133, il cui scopo è quello di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori, pubblici e privati, aventi una sede in Italia. La strategia del legislatore si concentra essenzialmente su tre punti chiave: la *cybersecurity*, la ricerca di competenze specifiche nel settore di riferimento e le linee di azione per l'attuazione delle disposizioni normative. In ossequio alla legislazione europea accennata, la legge 18 novembre 2019, n. 133, è caratterizzata anche dalla presenza di stringenti obblighi per gli operatori dei servizi essenziali, dei servizi digitali e delle imprese che forniscono reti pubbliche di comunicazioni e servizi di comunicazione elettronica accessibili al pubblico, inclusi nel perimetro di sicurezza nazionale cibernetica. Il primo dei quattro DPCM attuativi del Perimetro di sicurezza nazionale cibernetica è entrato in vigore il 5 novembre 2020[47] e stabilisce le macrocategorie di destinatari della sua disciplina, ossia, da un lato, i soggetti che esercitano una funzione essenziale dello Stato, vale a dire coloro i quali l'ordinamento attribuisce compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi

[45] DPCM 17 Luglio 2020, Approvazione Piano Triennale per l'informatica nella PA 2020-2022

[46] G. ZICCARDI, P. PERRI, *Tecnologia e diritto, Informatica giuridica avanzata*, Giuffrè Francis Lefebvre, Volume 3, 2019, p. 207-209

[47] DPCM 30 luglio 2020, n. 131, Regolamento in materia di perimetro di sicurezza nazionale cibernetica

ISSN 2036-7821

costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico, finanziario e dei trasporti, dall'altro, i soggetti che prestano un servizio essenziale per gli interessi dello Stato, ovvero qualsiasi soggetto, pubblico o privato, che presti un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato. Ciascuna amministrazione ha il compito dell'identificazione delle funzioni essenziali e dei servizi essenziali di diretta pertinenza, ovvero esercitati o prestati da soggetti vigilati o operatori anche privati, che dipendono da reti, sistemi informativi o servizi informatici e la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale. Le stesse predispongono una proposta di lista di questi operatori da sottoporre al Comitato Interministeriale per la Sicurezza della Repubblica (CISR) e al CISR tecnico. Nel caso in cui uno dei soggetti rientranti nei settori inclusi nel Perimetro fosse vittima di un attacco *cyber* sarà obbligato ad informare entro 6 ore al massimo lo CSIRT (*Computer Security Incident Response Team*), ovvero il gruppo di esperti istituito presso il DIS (Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri). La notifica, che può essere anche su base volontaria, verrà inoltrata alle autorità preposte: il Viminale e la presidenza del Consiglio per le notifiche di soggetti pubblici, il MISE per quelli privati. Si noti la differenza con il termine di 24 ore previsto dalla Direttiva NIS, lì dove si enuncia che per incidente si intende «ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici». In caso di grave violazione, scatta il coinvolgimento dell'NSC, il Nucleo per la sicurezza cibernetica, che proporrà al Presidente del Consiglio una possibile risposta all'attacco e coordinerà il ripristino del servizio. I principali punti di contatto con la disciplina *privacy* attengono alla valutazione delle conseguenze derivanti dalla perdita di disponibilità, integrità o riservatezza dei dati, la capacità di ripristino della disponibilità dei dati durante l'evento, l'applicazione dei principi di *privacy by design* e *privacy by default* nel trattare i dati dei soggetti inclusi nel Perimetro. I più recenti provvedimenti dell'esecutivo in tale ambito possono essere ricondotti nei due decreti del Presidente del Consiglio entrati in vigore il 14 gennaio del 2021[48], con cui si è

[48] DPCM 18 dicembre 2020, n. 179, Regolamento per l'individuazione dei beni e dei rapporti di interesse nazionale nei settori di cui all'articolo 4, paragrafo 1, del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, che individua i beni e rapporti di interesse nazionale in cui si applica il *Golden power* nei settori energia; acqua; salute; archiviazione, accesso e controllo di dati e informazioni sensibili; infrastrutture elettorali; settore finanziario, compreso quello creditizio e assicurativo e infrastrutture dei mercati finanziari; intelligenza artificiale, robotica, semiconduttori, cybersicurezza, nanotecnologie e biotecnologie; infrastrutture e tecnologie aerospaziali non militari; approvvigionamento di fattori produttivi critici in ambito siderurgico e del settore agroalimentare; prodotti a duplice uso (civile e militare); DPCM 23 dicembre 2020, n. 180, Regolamento per l'individuazione degli attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, a norma dell'articolo 2,

ISSN 2036-7821

definito il perimetro di competenza della normativa *Golden Power*. Il raccordo con la normativa sul cd. *Golden Power* in materia di apparati e tecnologie 5G, per gli aspetti relativi alla valutazione tecnica dei fattori di vulnerabilità, affidata al Centro di Valutazione e Certificazione Nazionale (CVCN), giocherà un ruolo fondamentale, così come l'assegnazione al Presidente del Consiglio di strumenti d'immediato intervento che consentano, su deliberazione del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), di affrontare con la massima efficacia e tempestività situazioni di rischio grave e imminente per la sicurezza nazionale in ambito *cyber*[49]. In definitiva, non possono negarsi i ritardi accumulati nel tempo e aggravati a causa dell'emergenza pandemica da Covid-19, tuttavia il Perimetro italiano, esperienza peculiare, ha suscitato interesse fuori dai confini nazionali, incassando l'importante apprezzamento del NIS *cooperation group* europeo e ponendo le premesse per la costruzione di un sistema all'avanguardia e, soprattutto, efficace. Si segnala tuttavia che, conscia di quanto il livello di cibersicurezza nel *business* sia ancora basso in tutta Europa, la Commissione Europea recentemente ha annunciato due nuove direttive sui temi della protezione delle infrastrutture critiche e della *cybersecurity*: la Direttiva NIS 2 e la Direttiva ICE. La prima, tesa a rimpiazzare la Direttiva NIS del 2016, individua alcuni settori strategici (energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione, spazio), ed altri definiti comunque "entità importanti", dunque degni di attenzione (servizi postali e corrieri, smaltimento rifiuti, manifattura, produzione e distribuzione di prodotti chimici, produzione, elaborazione e distribuzione di alimenti, manifattura, provider di servizi digitali), nel solco tracciato dal legislatore italiano con il Perimetro di sicurezza nazionale cibernetica, ai fini di un'armonizzazione nel panorama europeo in materia di cibersicurezza. Strettamente correlato a questa riforma è il tentativo, del legislatore europeo, di operare un lavoro di aggiornamento della Direttiva ICE 2, che revisiona la 114/08 sulle Infrastrutture critiche europee in materia di resilienza delle entità critiche rispetto a minacce fisiche, contemplando anch'essa un elenco di operatori e di settori essenziali da coinvolgere.

---

comma 1, del decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56, che individua gli attivi di rilevanza strategica nel sistema energetico nazionale nelle reti energetiche di interesse nazionale, e nei relativi rapporti convenzionali, includendovi: a) rete nazionale di trasporto del gas naturale e relative stazioni di compressione e centri di dispacciamento, come individuata ai sensi dell'articolo 9 del decreto legislativo 23 maggio 2000, n. 164, nonché gli impianti di stoccaggio del gas; b) infrastrutture di approvvigionamento di energia elettrica e gas da altri Stati, compresi gli impianti di rigassificazione di GNL *onshore* e *offshore*; c) rete nazionale di trasmissione dell'energia elettrica e relativi impianti di controllo e dispacciamento; d) attività di gestione e immobili fondamentali connessi all'utilizzo delle reti e infrastrutture di cui alle precedenti lettere a), b) e c).

[49] COMITATO INTERMINISTERIALE PER LA SICUREZZA DELLA REPUBBLICA (CISR), SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA 2019, *Documento di sicurezza nazionale*, Allegato alla *Relazione Annuale al Parlamento 2019*, p. 13

ISSN 2036-7821

3. Le nuove sfide nella gestione della cybersecurity.

La sicurezza delle informazioni e dei dati, in determinate realtà, è ancora percepita come mero adempimento, sia sotto il profilo economico sia sotto il profilo organizzativo. Appare necessario che le pubbliche amministrazioni e le Aziende interessate sviluppino sistemi di gestione del rischio che consentano di limitare i pericoli dell'interconnessione, mediante un'opera di sensibilizzazione e di rinnovamento, con il precipuo scopo di scongiurare il verificarsi di situazioni afflittive in merito alla sicurezza, con le relative conseguenze che ne potrebbero scaturire. La sicurezza dei dati, infatti, non deve essere percepita, come un aggravio economico, bensì come un *asset* indispensabile, considerato l'aumento esponenziale degli attacchi informatici degli ultimi anni. Si rende essenziale, allora, la pianificazione di strategie tecniche ed organizzative, mediante un lavoro basato sulla consapevolezza dei soggetti che operano con strumenti elettronici, nonché l'adozione di *policies* efficaci e mirate sessioni formative rivolte ai soggetti autorizzati. Negli ultimi anni, causa l'aumento dei *devices*, degli oggetti connessi mediante tecniche di intelligenza artificiale, e l'entrata in vigore negli ordinamenti giuridici europei dei principi contenuti nel Reg. UE 2016/679, le problematiche relative alla tutela dei dati personali sono salite alla ribalta dell'analisi accademica e politica, con una conseguente maggiore attenzione ai temi della *cybersecurity*. A tal riguardo, già nel Rapporto Clusit 2015[50] si leggeva che, sulla base di studi settoriali avviati su scala mondiale, diverse Organizzazioni, appartenenti a differenti settori merceologici, avevano subito un elevatissimo tasso di compromissione del proprio patrimonio informativo rilevante. La crescita del fenomeno negli ultimi anni, pertanto, angustia le amministrazioni pubbliche, alla luce della quantità e qualità delle risorse che gli attaccanti possono mettere in campo, con strategie e strumenti sofisticati finalizzati ad esfiltrare dati dei pubblici Uffici senza alcuna possibilità di difesa per questi ultimi[51]. Il legislatore europeo, nel 2016, ha optato allora per l'approccio "*Cybersecurity by Law*", scatenando la corsa alla "*compliance*" da parte di tutte le realtà produttive, la cui *mission* principale è quella di adottare, con il minimo sforzo, quelle "misure di sicurezza adeguate" che consentano di evitare i provvedimenti sanzionatori delle Autorità di controllo. Tutto ciò, inevitabilmente, può contribuire a diffondere un falso senso di sicurezza, poiché il termine "*compliance*" non coincide automaticamente con quello di *security*. Non a caso, il Reg. UE 2016/679 menziona le misure di sicurezza "adeguate", e alcuni eventi recenti insegnano che per gli Enti non può ritenersi sufficiente il generico rispetto delle norme in vigore per minimizzare il

[50] CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, Rapporto 2015 sulla sicurezza informatica in Italia, 2015, in https://clusit.it/pubblicazioni/.

[51] M. IASELLI, *Manuale operativo del D.P.O.*, Maggioli Editore, 2018, p. 105

ISSN 2036-7821

rischio di violazione[52]. Risulta di tutta evidenza il necessario ricorso alle competenze in *Identity and Access management* (IAM), *Secure Content and Threat Management* (SCTM), e in Sicurezza e gestione delle vulnerabilità[53]. A tal riguardo, preme ricordare che il tema della sicurezza delle informazioni non è legata soltanto alla riservatezza del dato, bensì anche alla sua disponibilità e alla sua integrità. Si pensi, infatti, ai frequenti attacchi "*ransomware*" sferrati agli Enti pubblici locali, che mettono a rischio la disponibilità dei servizi delle amministrazioni pubbliche, nonché al proliferare delle applicazioni mediche, la cui sicurezza desta più di una preoccupazione, in special modo, quando l'utilizzo delle stesse persegue le finalità di cura dei pazienti affetti da malattie croniche. Il *risk-based approach*, allora, pur non essendo il rimedio a tutti i mali, può assumere spessore, poiché misura il livello di rischio calcolando, rispettivamente, il parametro della probabilità di accadimento delle minacce e quello relativo alla gravità delle conseguenze (impatti sulle persone fisiche interessati). I risultati di tale impostazione generano benefici in merito alla minimizzazione degli episodi di violazione di dati personali. In ipotesi, il *data breach*, che consegue agli incidenti di sicurezza sui dati personali, infatti, può condurre alla configurazione di danni di natura sociale, reputazionale ed economica, in considerazione del limitato arco di tempo a disposizione del titolare del trattamento per difendersi adeguatamente (e, quindi, tentare di rimediare all'evento). Senza contare che, se l'incidente di sicurezza riguarda anche dati personali, ai sensi dell'art. 33 Reg. UE 2016/679, il titolare del trattamento, entro 72 ore dal momento in cui è venuto a conoscenza dell'evento, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone, deve procedere alla notifica al Garante. Invero, non va trascurato che, nella perdurante fase emergenziale da Covid-19, il rischio associato alla grande diffusione del telelavoro ha "ingolosito" i criminali informatici. Più in generale, secondo il *Cybermalveillance* (iniziativa del governo francese per rispondere al numero crescente di atti *cyber*-dannosi) gli strumenti di attacco più diffusi, ad oggi, sono rappresentati dal *phishing* e dal *ransomware*, vale a dire tecniche di furto di dati e organizzazione di falsi ordini di trasferimento, allo scopo di sottrarre credenziali e dati, e di mettere in atto un sistema di frodi, creando un danno all'attività e all'immagine dell'azienda o dell'organizzazione[54]. Appare chiaro quanto sia preziosa, in tal senso, la previsione,

[52] Con una Nota del 2 aprile 2020, il Garante per la protezione dei dati personali ha comunicato di aver avviato un'istruttoria, a seguito delle numerose segnalazioni pervenute e della notifica di data breach effettuata dall'INPS e che ha riguardato il suo sito istituzionale, allo scopo di effettuare opportune verifiche e valutare l'adeguatezza delle contromisure adottate dall'Ente e gli interventi necessari a tutelare i diritti e le libertà degli interessati.

[53] D. BENEDETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, 2018, pp. 261-263.

[54] PUBLIC INTEREST GROUPING ACTION AGAINST CYBERMALVEILLANCE (GIP ACYMA), *Recommandations de sécurité informatique pour le télétravail en situation de crise*, 23 marzo 2020, in https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail.

ISSN 2036-7821

sulla base dell'articolazione degli Uffici degli Enti pubblici e delle Organizzazioni, di un processo di *Incident Response*, e, conseguentemente, l'elaborazione, *by design*, di una *policy* utile alla gestione dell'evento di *data breach*, mediante la composizione di una dedicata "unità di crisi" e una netta ripartizione dei ruoli dei protagonisti chiamati in causa.

4. Due figure fondamentali: il responsabile protezione dati e il responsabile per la transizione al digitale.

Sulla base del contesto rappresentato, emerge con forza l'importanza della nomina di un responsabile protezione dati (o *data protection officer*), anche laddove tale nomina non sia obbligatoria. Il legislatore europeo in materia di protezione dati, orbene, ha introdotto nel *corpus* normativo, all'art. 37, Reg. UE 2016/679, tale figura, da designare obbligatoriamente dal titolare del trattamento e dal responsabile del trattamento ogniqualvolta il trattamento sia effettuato da un'Autorità pubblica o da un organismo pubblico, quando le attività principali del titolare del trattamento o del responsabile del trattamento consistano in trattamenti che, per loro natura, ambito di applicazione e finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala, o, ancora, se le attività principali del titolare del trattamento o del responsabile del trattamento si concretizzino nel trattamento, su larga scala, di categorie particolari di dati o di informazioni relative a condanne penali e a reati. Se ne desume che, alla luce delle novità precedentemente evidenziate, il legislatore europeo sembra affidare al responsabile protezione dati un ruolo di garanzia della *compliance*, alla stregua di un "garante interno"[55], lì dove le disposizioni rilevanti in materia richiamano il titolare e il responsabile al tempestivo ed adeguato coinvolgimento del *data protection officer* in tutte le questioni che possono impattare sui diritti e le libertà fondamentali degli interessati. La selezione di quest'ultimo, come richiamato più volte dal Garante per la protezione dati[56], deve tenere conto delle competenze giuridiche, informatiche e manageriali maturate, della conoscenza tecnica del contesto in cui opera il titolare del trattamento e, specialmente, della capacità di assolvere ai propri compiti e promuovere la cultura della protezione dei dati all'interno dell'organizzazione. I compiti del *data protection officer*, tracciati nell'art. 38, Reg. UE 2016/679, sono essenzialmente finalizzati a sorvegliare l'osservanza della normativa in materia, informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai soggetti autorizzati che, operativamente, eseguono le operazioni di trattamento. Ne deriva che al responsabile

[55] N. BRUTTI, *Le figure soggettive delineate dal GDPR, la novità del Data Protection Officer*, in *Privacy digitale*, a cura di Emilio Tosi, Giuffré, 2019, p. 149

[56] GARANTE PER LA PROTEZIONE DATI PERSONALI, *Quesiti in materia di certificazione delle competenze ai fini della prestazione di consulenza in materia di protezione dei dati personali*, 28 luglio 2017, in https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7057222

ISSN 2036-7821

protezione dati è demandato il compito di "rappresentare" il titolare del trattamento in tutte quelle attività che richiedono la cooperazione con l'Autorità di controllo e ogni ulteriore interlocuzione formale con la stessa per questioni connesse al trattamento, tra cui la consultazione preventiva, espressamente prevista dall'art. 36 del Regolamento. Ulteriore compito afferente al responsabile della protezione dati è quello di rilasciare un parere (e sorvegliarne lo svolgimento) in ordine alla valutazione d'impatto sulla protezione dei dati. In tal senso, quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, infatti, ai sensi dell'art. 35 Reg. UE 2016/679, il titolare, sin dalla fase di progettazione, effettua una valutazione dell'impatto sulla protezione dei dati personali in ordine alle operazioni di prossima attuazione (*Data Protection Impact Assessment*), procedura tecnica che tratteggia gli elementi essenziali delle operazioni di trattamento, finalizzata a valutare e a prevedere, all'esito, l'adozione di misure tecniche necessarie a preservare le libertà fondamentali degli interessati. Sono state individuate, sotto un profilo più operativo, delle attività imprescindibili per il responsabile protezione dati nell'esercizio della propria funzione[57]. Tale figura, che deve avere un'approfondita conoscenza di tutti gli aspetti organizzativi dell'organizzazione, anzitutto ha un ruolo di supervisione su una serie di attività del titolare del trattamento quali la mappatura dei trattamenti, attraverso la diretta compilazione del registro delle operazioni di trattamento, ai sensi dell'art. 30, Reg. UE 2016/679, l'individuazione di un organigramma *privacy*, la formazione dei soggetti autorizzati dal titolare, la redazione di specifiche *policies* del trattamento dei dati, la predisposizione di un'efficace strategia in materia di sicurezza informatica, la predisposizione di procedure in caso di *data breach*, la gestione degli audit interni ed esterni. In secondo luogo il responsabile protezione dati cura i rapporti con gli interessati e con l'Autorità Garante, nonché il proprio aggiornamento professionale[58]. Di tal guisa, si può affermare che non si è ancora compresa fino in fondo, nel settore pubblico come nel settore privato, l'importanza della figura del *data protection officer*. Eppure, la designazione di un responsabile per la protezione dati genera benefici sia in termini di sicurezza dei trattamenti, ponendo al riparo le amministrazioni dal rilevante impianto sanzionatorio, sia sotto il profilo puramente giuridico. In primo luogo poiché, per gli Enti pubblici, sarebbe grave la mancata adozione degli adempimenti normativi nella gestione dei rapporti con le terze parti cui vengono affidati servizi che implicano il trattamento di dati personali degli interessati, stante l'obbligo

[57] A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione*, Rivista di diritto amministrativo, Amministrativ@mente, Numero 5-6, 2018, pp. 19-21.

[58] F. LORÈ, *Il ruolo del Responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del Regolamento generale sulla protezione dei dati personali UE 2016/679*, Rivista di diritto amministrativo, Amministrativ@mente, Numero 7-8, 2018, pp. 12-14.

ISSN 2036-7821

cogente della nomina del responsabile del trattamento nei casi di esternalizzazione delle attività di trattamento dei dati. L'art. 28, par. 3, Reg. UE 2016/679, difatti, impone che i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Inoltre, non può essere taciuto che la mancata nomina del responsabile protezione dati pone in pericolo il bilanciamento tra le contrapposte esigenze di trasparenza amministrativa e di tutela della riservatezza, rischiando di incrinare il rapporto pubblica amministrazione - cittadino, sia con riferimento ai procedimenti di accesso documentale e civico[59], sia con riferimento agli obblighi di pubblicità e trasparenza sui siti web istituzionali[60]. Per quel che concerne quest'ultimo aspetto, preme ricordare che, negli ultimi anni, il Garante è intervenuto con numerose ordinanze di ingiunzione a causa della mancata applicazione del principio di minimizzazione del dato in tema di pubblicità e trasparenza *online*. Siffatti interessi inducono, sotto altro profilo, a fare breve cenno anche alle importanti funzioni del responsabile per la transizione al digitale, figura prevista, a partire dal 14 settembre 2016, con le modifiche operate dal legislatore al CAD. Pur essendo essa obbligatoria, tuttavia, molte amministrazioni non hanno provveduto immediatamente ad adeguarsi, tanto che si è resa necessaria una Circolare del Ministro per la Pubblica Amministrazione[61], per sollecitare l'individuazione di un responsabile per la transizione al digitale. Nella Circolare *de qua*, il Ministro ricorda come rivesta particolare rilievo, nell'ambito della serie di azioni governative per la trasformazione digitale della pubblica amministrazione, la figura del responsabile, strategica nel percorso di digitalizzazione del Paese[62]. Difatti, a tenore dell'art. 17, comma 1, CAD, ciascuna amministrazione è tenuta ad affidare ad un unico ufficio dirigenziale la «transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità». Si tratta di un ufficio, non necessariamente "fisico", cui sono assegnati compiti di riorganizzazione interna per il raggiungimento degli scopi del CAD. Laddove impossibilitata alla creazione *ex-novo* dell'ufficio del responsabile, la

[59] D. U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e Pubblica Amministrazione: un'analisi storico-evolutiva in una prospettiva di diritto comparato ed europeo*, in *Rivista italiana di diritto pubblico comunitario*, 2016, p. 1019 ss.

[60] R. SCIAUDONE, E. CARAVÀ (a cura di), *Il Codice della Privacy, Commento al D.lgs 30 gugno 2003, e al D.Lgs. n.101/2018, alla luce del Regolamento UE 2016/679 (GDPR)*, Pacini Giuridica, 2019, pp. 86-92

[61] MINISTERO PER LA PUBBLICA AMMINISTRAZIONE, Circolare n. 3 del 1 ottobre 2018.

[62] F. MARTINES, *La digitalizzazione della pubblica amministrazione*, Rivista di Diritto dei Media, MediaLaws, Numero 2/2018, pp. 152-154.

ISSN 2036-7821

pubblica amministrazione può far coincidere tale funzione con un ufficio già esistente, e in tali casi, il responsabile per la transizione al digitale corrisponderebbe con il responsabile dell'ufficio prescelto. Con riguardo ai compiti più stringenti del responsabile, pertanto, oltre ad una preliminare analisi della situazione nell'ambito della transizione al digitale della pubblica amministrazione di riferimento, con annessa mappatura dei flussi procedimentali, tale figura è chiamata a riorganizzare, sotto il profilo tecnico, i processi amministrativi, a programmare e a coordinare gli interventi necessari in materia di sicurezza informatica, a trasformare l'amministrazione di appartenenza al fine di renderla aperta e accessibile, e a curare i canali di comunicazione digitali e il sito web istituzionale. Sulla scorta di quanto sin qui rappresentato, al responsabile per la transizione al digitale, che ha un ruolo gerarchicamente superiore a ogni altro dirigente nell'attuazione di tutte le iniziative legate al digitale, spetta il coordinamento delle attività previste dal CAD, che riguardano i diritti "digitali" dei cittadini e la "digitalizzazione" dei processi della pubblica amministrazione, quali il coordinamento strategico dello sviluppo dei sistemi informativi e di telecomunicazione, l'accesso dei soggetti disabili agli strumenti informatici, la promozione dell'accessibilità, il miglioramento della soddisfazione dell'utenza e della qualità dei servizi, nonché la riduzione dei tempi e dei costi dell'azione amministrativa, e la diffusione, all'interno dell'amministrazione, dei sistemi di protocollo informativo, di firma digitale e di identità, e di domicilio digitale. Nondimeno, al responsabile per la transizione al digitale è demandato il compito di pianificare, coordinare e monitorare le misure a presidio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture, in applicazione delle misure minime di sicurezza AgID per la pubblica amministrazione[63], anche se oggi, queste misure, con l'incedere della tecnologia e alla luce del nuovo quadro normativo in materia di protezione dati e di *cybersecurity*, appaiono quantomeno bisognevoli di aggiornamento. Ne discende, dunque, che il responsabile per la transizione debba essere dotato di adeguate competenze tecnologiche, manageriali e, soprattutto, in materia di informatica giuridica. Considerato che uno degli elementi fondanti del Reg. UE 2016/679 è il principio di sicurezza del trattamento, è auspicabile la collaborazione tra *data protection officer* e responsabile per la transizione al digitale, al fine di assicurare la *compliance* normativa. Va segnalato, tuttavia, che la pubblica amministrazione paga la mancanza di competenze specifiche in questo ambito e sovente si riscontra l'oggettiva impossibilità nell'individuare il soggetto apicale cui affidare le funzioni di responsabile per la transizione al digitale, non essendo così diffuse le *skills* digitali, complicazione che diventa drammatica negli Enti pubblici di piccole dimensioni, nei quali, spesso, si hanno a disposizione poche unità in termini

[63] AgID, CIRCOLARE 18 aprile 2017, n. 2. Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

ISSN 2036-7821

di risorse umane. *Rebus sic stantibus*, per non correre il rischio di avere un ottimo impianto normativo che non troverà, però, uniforme applicazione per molti anni ancora, dovrà essere il legislatore a ricercare, allora, una soluzione che imponga l'avvio di un percorso di formazione tecnica negli ambiti richiamati, o in alternativa, la definizione di un accordo che consenta ai tanti specialisti che non sono nelle dotazioni organiche delle amministrazioni pubbliche di dare il proprio contributo nel passaggio al digitale e, più in generale, in tutte le sfide che la tecnologia porta con sé, spesso foriere di un più appropriato esercizio dei diritti da parte dei cittadini.

5. Conclusioni.

In definitiva, evidenziato il panorama normativo, appare, *ictu oculi,* evidente la necessità non soltanto un riallineamento delle misure di *security*, ma anche una gestione proattiva dei processi e una sensibilizzazione dell'intero personale, con un'efficace *governance* della sicurezza informatica, di non facile realizzazione per molte realtà. Lo standard ISO / IEC 27001 definisce la *governance IT* come il sistema mediante il quale un'organizzazione dirige e controlla la *governanc*e della sicurezza, specifica il quadro di responsabilità e fornisce supervisione utile a garantire che i rischi siano adeguatamente mitigati, mentre la direzione assicura che i controlli siano implementati per mitigare i rischi. Come osservato, gli scopi da raggiungere per controllo efficace si possono sintetizzare in cinque sfide fondamentali[64]. La prima sfida è la definizione chiara, da parte dell'organizzazione, delle proprie politiche, strategie e obiettivi di gestione del rischio. Una buona strategia è preordinata a definire, appropriatamente, la correlazione del rischio alle operazioni aziendali critiche, lo sviluppo di obiettivi strategici per l'organizzazione, le esigenze in termini di sicurezza informatica, gli indicatori chiave di prestazione, il fabbisogno di risorse, la propensione al rischio e i metodi di monitoraggio continuo[65]. La seconda sfida si sostanzia nel creare processi standardizzati, senza i quali le organizzazioni non possono garantire efficienza, qualità e coerenza. Un programma di controllo della sicurezza informatica ad *hoc* e incoerente finirà per portare a profonde carenze infrastrutturali, così come un programma di *governance* inefficace condurrà a maggiori violazioni, compromissioni e attacchi della sicurezza. Con riferimento alla terza sfida, la *governance* della sicurezza informatica dovrebbe comporre un sistema di responsabilità per la conformità a tutti i livelli del personale. Il *National Institute of Standards and Technology* (NIST), nel proprio *Risk Management Framework* (RMF), a tal riguardo, ha delineato un insieme di linee guida finalizzate a stabilire come le organizzazioni possono prevenire, rilevare e rispondere agli attacchi

[64] S. SWINTON (Carnegie Mellon University, Pittsburgh), *Cybersecurity Governance, Part 1: 5 Fundamental Challenges*, 25 luglio 2019, in *https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html.*

[65] S. SWINTON, *Ibidem*

ISSN 2036-7821

informatici[66], raccomandando un approccio a più livelli nella gestione del rischio e promuovendo lo sviluppo di funzionalità di sicurezza e *privacy* nei sistemi informativi, durante l'intero ciclo di vita dello sviluppo del sistema. La quarta sfida si concretizza nell'implementazione di una "supervisione" della *leadership senior*, secondo standard elevati[67]. A tal fine, ed in questo consiste la quinta sfida, proprio la *leadership senior* deve garantire risorse adeguate per soddisfare le esigenze di *governance* e di conformità della sicurezza informatica, commisurate alla strategia dell'organizzazione, e destinate, altresì, all'*empowerment* del personale dipendente delle Organizzazioni[68]. Come riportato dal Rapporto Clusit 2020[69], «si è oltrepassato un punto di non ritorno, tale per cui ormai ci troviamo a vivere ed operare in una dimensione differente, in una nuova epoca, in un "altro mondo", del quale ancora non conosciamo bene la geografia, gli abitanti, le regole e le minacce. Gli attaccanti non sono più "*hackers*", e nemmeno gruppetti effimeri (più o meno pericolosi) di "artigiani" del *cybercrime*: sono decine e decine di gruppi criminali organizzati transnazionali che fatturano miliardi, multinazionali fuori controllo dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, i loro fornitori e *contractors*, gruppi *state-sponsored* civili e paramilitari, ed unità di mercenari impegnati in una lotta senza esclusione di colpi, che hanno come campo di battaglia, arma e bersaglio le infrastrutture, le reti, i *server*, i *client*, i *device* mobili, gli oggetti *internet of things*, le piattaforme *social* e di *instant messaging* (e la mente dei loro utenti), su scala globale. Una situazione di inaudita gravità, che mette in discussione ed a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi (*online* e *offline*) che su di essa fanno affidamento». A fronte di tutto ciò, si segnala che di recente il NIST ha pubblicato la versione ufficiale del *Framework* NIST SP 800-53 Rev. 5[70], aggiornata il 10 dicembre

[66] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, *FISMA Implementation Project*, in https://csrc.nist.gov/projects/risk-management/rmf-overview.

[67] Lo standard ISO 27001, alla Sezione 5, contiene un elenco di principi di leadership rilevanti per stabilire un efficace programma di governance della sicurezza informatica: assicurare che la politica di sicurezza delle informazioni e gli obiettivi di sicurezza delle informazioni siano stabiliti e siano compatibili con la direzione strategica dell'organizzazione; garantire che i requisiti del sistema di gestione della sicurezza delle informazioni siano integrati nei processi dell'organizzazione; assicurare che le risorse necessarie per il sistema di gestione della sicurezza delle informazioni siano disponibili; comunicare l'importanza di una gestione efficace della sicurezza delle informazioni e conformarsi ai requisiti del sistema di gestione della sicurezza delle informazioni; garantire che il sistema di gestione della sicurezza delle informazioni raggiunga i risultati previsti; dirigere e supportare il personale per contribuire all'efficacia del sistema di gestione della sicurezza delle informazioni; promuovere continui miglioramenti.

[68] S. SWINTON, (Carnegie Mellon University, Pittsburgh), *Cybersecurity Governance, Part 1: 5 Fundamental Challenges*, 25 luglio 2019, in https://insights.sei.cmu.edu/insider-threat/2019/07/cybersecurity-governance-part-1-5-fundamental-challenges.html

[69] CLUSIT – ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, *Rapporto CLUSIT 2020*, edizione di marzo 2020, in https://clusit.it/pubblicazioni/, p. 7

[70] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*, 2020, in https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

2020, un insieme di "famiglie" di controlli di sicurezza integrati con la *privacy*. Il «Framework nazionale per la *cybersecurity* e la *data protection*» italiano, di diretta derivazione dell'originaria formulazione, è già obbligatorio per gli Operatori di servizi economici essenziali (OES/OSE) della normativa NIS. Le famiglie di controlli cui si fa riferimento sono diverse, quali quelle sul controllo degli accessi, sugli audit e sulle responsabilità, sulla pianificazione di emergenza, e sulla protezione fisica e ambientale. In conclusione, alla luce, anche, del recentissimo *NIS Investments Report* di ENISA[71], che ha svolto un'indagine su 251 organizzazioni in cinque Stati membri dell'UE in merito alle risorse destinate ad "investimenti NIS", dalle cui risultanze è emerso come nell'Unione si investa, nel settore *cybersecurity*, circa il 40% in meno degli Stati Uniti, con un rilevante impatto finanziario dei danni conseguenti ad attacchi informatici, si può affermare che emerge con forza la necessità di un cambiamento culturale, nel settore pubblico e in quello privato, che consenta di destinare, "di default", maggiori risorse economiche alla protezione dei dati personali e alla *cybersecurity*, in un'ottica di prevenzione del rischio e non di riparazione del danno.

[71] ENISA, *NIS Investments Report*, 2020, in https://www.enisa.europa.eu/publications/nis-investments/.