dirittifondamentali.it

Dirittifondamentali.it - Fascicolo 2/2020
Data di pubblicazione – 18 maggio 2020

La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*.

di
Barbara Borrillo*

SOMMARIO: 1. Premessa. – 2. Il modello sanzionatorio dopo l'introduzione del GDPR. – 3. Le sanzioni inflitte dalle Autorità di controllo dell'Unione europea. In particolare le sanzioni inflitte dal Garante italiano: i c.dd. casi Rousseau e Tim s.p.a. – 4. Le nuove tecnologie e l'*e-voting*. – 5. Il principio di *accountability*. – 6. Rilievi conclusivi.

1. Premessa

«Anche se è eccessivo, e persino pericoloso dire che noi siamo i nostri dati, è tuttavia vero che la nostra rappresentazione sociale è sempre più affidata a informazioni sparse in una molteplicità di banche dati, e ai profili che su questa base vengono costruiti, alle simulazioni che permettono. Siamo sempre più conosciuti da soggetti pubblici e privati attraverso i dati che ci riguardano, in forme che possono incidere sull'eguaglianza, sulla libertà di comunicazione, di espressione o di circolazione, sul diritto alla salute, sulla condizione di lavoratore, sull'accesso al credito e alle assicurazioni, e via elencando. Divenute entità disincarnate, le persone hanno sempre di più bisogno di una tutela del loro corpo elettronico»[1].

Queste parole di Stefano Rodotà forniscono un sintetico e al tempo stesso esaustivo scenario del rapporto tra le tecnologie dell'informazione e della comunicazione e la *privacy*[2]. Ed è proprio su tale scenario che la presente indagine intende focalizzare la

* Ricercatore di Diritto privato, Università degli studi di Bari Aldo Moro, sede di Taranto.
*Intervento programmato predisposto per il Convegno «*Tecnologie digitali, protezione dei dati personali e diritto del lavoro*», Dipartimento DEMM, Università degli studi del Sannio, Benevento.
[1] S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 395.
[2] I contributi sul tema dell'influenza delle nuove tecnologie sulla *privacy* sono numerosissimi. Senza pretesa di esaustività si citano i seguenti contributi: S. RODOTÀ, *Persona. Riservatezza.*

propria attenzione, ponendo come principale oggetto di studio due tematiche, tra loro saldamente connesse, che ben si coordinano con lo scenario prospettato: l'impatto del GDPR[3] in materia di tutela dei dati personali e il sistema sanzionatorio dallo stesso novellato. Due i profili del sistema sanzionatorio al centro dell'analisi: quello teorico, relativo alle novelle introdotte dal regolamento europeo e quello applicativo, riguardante le sanzioni amministrative irrogate dalle Autorità di controllo dell'Unione Europea successivamente alla entrata in vigore della nuova disciplina – sanzioni irrogate a fronte dell'utilizzo poco avveduto delle nuove tecnologie. L'obiettivo è quello di fornire una risposta, quanto più possibile ponderata e attendibile, al delicato quesito della idoneità del reg. UE 4 maggio 2016, n. 679 di perseguire l'intento, largamente sponsorizzato nei suoi Considerando, di rinvigorire la tutela del diritto alla riservatezza. È di tutta evidenza che tale quesito non può trovare risposta mediante l'analisi del solo profilo sanzionatorio: tuttavia, lo studio dello stesso rappresenta un

Identità. Prime note sistematiche sulla protezione dei dati personali, in *Riv. crit. dir. priv.*, 1984, p. 583 ss.; E. ROPPO, *Informatica e tutela della* privacy *e diritti di libertà*, in G. ALPA (a cura di), Computers *e responsabilità civile*, Milano, 1985; G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, II, p. 313 ss.; S. RODOTÀ,*Tecnologie e diritti*, Bologna, 1995; G. CIACCI, *La tutela dei dati personali su Internet*, in A. LOIODICE e G. SANTANIELLO (a cura di), *La tutela della riservatezza*, in *Tratt. dir. amm.* Santaniello, Padova, 2000, p. 369 ss.; V. CARIDI, *La tutela dei dati personali in internet*: *la questione dei* logs *e dei* cookies *alla luce delle dinamiche economiche dei dati personali*, in *Dir. inf.*, 2001, p. 768 ss.; G. RESTA, *Identità personale e identità digitale*, *ivi*, 2007, p. 512 ss.; M.L. GAMBINI, *Dati personali e internet*, in *Quad. Rass. dir. civ.*, Napoli, 2008; M. CARTA, *Diritto alla vita privata ed internet nell'esperienza giuridica europea ed internazionale*, in *Dir. inf.*, 2014, p. 1 ss.; S. RODOTÀ, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014; A.C. NAZZARO, *L'utilizzo dei* Big data *e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, 4, p. 1241 ss.

[3] I contributi sul nuovo Regolamento sono a dir poco numerosi: tra i tanti si ricordano L. BOLOGNINI, E. PELINO e C. BISTOLFI, *Il Regolamento* Privacy *europeo*, Milano, 2016; F. PIZZETTI, Privacy *e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; M.G. STANZIONE, *Il Regolamento europeo sulla* privacy: *origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, 4, p. 1249 ss.; S. SICA, V. D'ANTONIO e G.M. RICCIO, *La nuova disciplina europea della* privacy, Padova, 2016; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, 2017; A. CICCIA MESSINA e N. BERNARDI, Privacy *e regolamento europeo*, Assago, 2017; M. MAGLIO, M. POLLINI e N. TILLI, *Manuale di diritto alla protezione dei dati personali. La* privacy *dopo il Regolamento UE 2016/679*, Santarcangelo di Romagna, 2017; M. SOFFIENTINI, *Protezione e trattamento dei dati*, Assago, 2018; G.M. RICCIO, G. SCORZA e E. BELISARIO (a cura di), *Gdpr e normativa* privacy. Commentario, Assago, 2018; G. FINOCCHIARO, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; E. TOSI, Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Milano, 2019.

profilo, oltre che imprescindibile, decisamente rilevante nella costruzione del *puzzle* dell'impatto della nuova disciplina in materia di protezione dei dati personali.

2. *Il modello sanzionatorio dopo l'introduzione del GDPR.*

Come è noto, il modello sanzionatorio della nuova disciplina[4] è descritto nell'art. 83 reg. UE n. 679 del 2016 – il quale determina le condizioni generali per l'applicazione di sanzioni amministrative pecuniarie da parte delle Autorità di controllo[5] – e nel nuovo

[4] Sul tema v., tra gli altri, E.A. MATARAZZO, *L'aspetto sanzionatorio della nuova legge sulla* privacy, in *Stato civ. it.*, 2018, 12, p. 57 ss.; D. TROMBINO, *Il GDPR verso il suo primo anno di vita. Informativa, trasferimento transnazionale e sanzioni*, in *Disc. comm. serv.*, 2019, 2, p. 43 ss.

[5] Per completezza si riporta il testo integrale dell'articolo in esame rubricato *Condizioni generali per infliggere sanzioni amministrative pecuniarie*: «1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive. 2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, § 2, lett. da *a* a *h* e *j*, o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi: a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito; b) il carattere doloso o colposo della violazione; c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli artt. 25 e 32; e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento; f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; g) le categorie di dati personali interessate dalla violazione; h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; i) qualora siano stati precedentemente disposti provvedimenti di cui all'art. 58, § 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti; j) l'adesione ai codici di condotta approvati ai sensi dell'art. 40 o ai meccanismi di certificazione approvati ai sensi dell'art. 42; e k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione. 3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione piú grave. 4. In conformità del § 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli artt. 8, 11, da 25 a 39, 42 e 43; b) gli obblighi dell'organismo di certificazione a norma degli artt. 42 e 43; c) gli obblighi dell'organismo di controllo a norma dell'art. 41, § 4; 5. In conformità del § 2, la violazione delle

art. 166 d.lg. 30 giugno 2003, n. 196[6] (c.d. codice *privacy*), così come modificato dal d.lg. 10 agosto 2018, n. 101[7], il quale prevede una serie di ulteriori fattispecie di illeciti soggetti alle sanzioni amministrative di cui al predetto art. 83[8].

---

disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore: a) i princípi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5, 6, 7 e 9; b) i diritti degli interessati a norma degli artt. da 12 a 22; c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli artt. da 44 a 49; d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX; e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'art. 58, § 2, o il negato accesso in violazione dell'articolo 58, § 1. 6. In conformità del § 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'art. 58, § 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. 7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'art. 58, § 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro. 8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo. 9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al piú tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica».

[6] In G.U. n. 174 del 29 luglio 2003, Suppl. Ord. n. 123.

[7] Recante "*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)*", in G.U. n. 205 del 4 settembre 2018.

[8] Di séguito il testo completo dell'art. 166 rubricato *Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori*: «1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, § 4, del Regolamento le violazioni delle disposizioni di cui agli artt. 2 *quinquies*, comma 2, 2 *quinquiesdecies*, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132 *ter*. Alla medesima sanzione amministrativa è soggetto colui che non effettua la valutazione di impatto di cui all'art. 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma. 2. Sono soggette alla sanzione amministrativa di cui all'art.o 83, § 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2 *ter*, 2 *quinquies*, comma 1, 2 *sexies*, 2 *septies*, comma 8, 2 *octies*, 2 *terdecies*, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110 bis, commi 2 e 3, 111, 111 *bis*, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132 *bis*, comma

Tale ultima disposizione distingue due gruppi di sanzioni amministrative. Da un lato, le violazioni c.dd. di minore gravità, per le quali sono previste le sanzioni amministrative pecuniarie di importi fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e riguardano, nello specifico, le violazioni degli obblighi imposti ai titolari e responsabili del trattamento, all'organismo di certificazione Accredia e all'organismo di controllo dei codici di condotta. Dall'altro lato, le violazioni c.dd. di maggiore gravità, per le quali sono previste sanzioni di importi fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, e

---

2, 132 *quater*, 157, nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2 *septies* e 2 *quater*. 3. Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, § 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'art. 83 del medesimo Regolamento e di cui ai commi 1 e 2. 4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a séguito di reclamo ai sensi dell'art. 77 del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'àmbito dell'esercizio dei poteri d'indagine di cui all'art. 58, § 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante. 5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attività di cui al comma 4 configurino una o piú violazioni indicate nel presente titolo e nell'art. 83, §§ 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare. 6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità. 7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 3 si osservano, in quanto applicabili, gli artt. da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'art. 156, comma 8, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento svolte dal Garante. 8. Entro il termine di cui all'art. 10, comma 3, del d.lg. n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata. 9. Nel rispetto dell'art. 58, § 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformità ai princípi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonché della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione. 10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'art. 83 del Regolamento non si applicano in relazione ai trattamenti svolti in àmbito giudiziario».

riguardano nello specifico le violazioni dei princípi di base del trattamento – comprese le condizioni relative al consenso –, dei diritti degli interessati, dei trasferimenti di dati personali a un destinatario in un Paese terzo o un'organizzazione internazionale, di qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX, nonché l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'Autorità di controllo o il negato accesso in violazione dell'articolo 58, § 1, GDPR.

L'art. 166 del codice *privacy*, oltre a prevedere i princípi e le modalità procedurali che il Garante dovrà rispettare nell'adozione dei provvedimenti sanzionatori, individua ulteriori fattispecie di illeciti soggetti alle sanzioni amministrative previste dalla disciplina comunitaria: sono sottoposti alla sanzione fino a 10 milioni di euro o al 2% del fatturato dell'impresa le violazioni delle disposizioni relative all'informativa da rendere con linguaggio semplificato rilasciata ai minori di quattordici anni in occasione dell'offerta diretta di servizi della società dell'informazione, ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che presentano rischi elevati, alle cartelle cliniche e ai certificati di assistenza al parto, ai trattamenti posti in essere dai fornitori di reti pubbliche di comunicazioni o di servizi di comunicazione elettronica accessibili al pubblico, alle attività di ricerca medica, biomedica ed epidemiologica. Andranno incontro alla più pesante sanzione fino a 20 milioni di euro o al 4% del fatturato dell'impresa coloro i quali violeranno le disposizioni sui trattamenti svolti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sulla raccolta del consenso prestato dai minori di quattordici anni in occasione dell'offerta diretta di servizi della società dell'informazione, sul trattamento di particolari categorie di dati per motivi di interesse pubblico rilevante, sulle procedure di accesso fisico e logico ai dati genetici, biometrici, relativi alla salute e a condanne penali e reati, sui diritti delle persone decedute, sulla diffusione di provvedimenti giudiziari contenenti dati personali, sui dati personali degli studenti, sui trattamenti a fini statistici, di ricerca scientifica e nell'àmbito di lavoro, in relazione alle assicurazioni, ai servizi di comunicazione elettronica nonché la violazione delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2 *septies* e 2 *quater* del codice.

L'effetto principale della nuova disciplina è stato quello di un deciso inasprimento delle sanzioni, con il fine, sottolineato da alcuni autori in dottrina[9], di incidere, in particolare, sulle condotte dei grandi gruppi multinazionali che trattano dati in diverse aree geografiche e spesso cercano di individuare i paradisi legali del trattamento dei dati personali per eludere norme e criteri di comportamento definiti dalle nazioni più rigorose.

Va chiarito preliminarmente che è stato, per così dire, concesso un periodo di tolleranza – rispettato dai Garanti europei – in merito all'adeguamento alla nuova normativa sulla protezione dei dati personali e all'applicazione delle sanzioni, giustificato dalla necessità di consentire alle imprese di adeguarsi alle novità del GDPR[10]. Tale previsione è stata senz'altro opportuna se appena si pensa alla circostanza, sulla quale si tornerà più avanti[11], che le modifiche introdotte dalla disciplina comunitaria inseriscono un vero e proprio procedimento di responsabilizzazione dei titolari e dei responsabili del trattamento: la *privacy*, da obiettivo secondario da perseguire mediante il rispetto di adempimenti formali, diventa il presupposto ineluttabile delle attività di trattamento. Di conseguenza, l'attuazione delle prescrizioni imposte dalla nuova normativa non può avvenire soltanto mediante l'adozione di misure formali (quali, ad esempio, l'adeguamento delle informative) bensì attraverso un *modus operandi* che deve diventare parte integrante dell'attività ordinaria.

3. Le sanzioni inflitte dalle Autorità di controllo dell'Unione europea. In particolare le sanzioni inflitte dal Garante italiano: i c.dd. casi Rousseau e Tim s.p.a.

Poste le premesse teoriche del nuovo impianto sanzionatorio, è opportuno analizzare quello che in apertura di indagine si è definito il profilo applicativo: il modo

[9] M. MAGLIO, *Il Regolamento europeo 2016/679 in materia di dati personali: inquadramento generale e prospettive di sviluppo*, in ID., M. POLLINI e N. TILLI, *Manuale di diritto alla protezione dei dati personali. La* privacy *dopo il Regolamento UE 2016/679*, cit., p. 67.

[10] In Italia l'art. 22, comma 13, d.lg. 101/2018 ha previsto che «[p]er i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie».

[11] V. *infra*, § 5.

migliore per tentare di rispondere al quesito con il quale si è esordito è quello di considerare i casi sottoposti all'attenzione delle Autorità di controllo dell'Unione europea e le sanzioni dalle stesse comminate.

L'entrata in vigore del nuovo Regolamento ha determinato un totale cambiamento nell'approccio adottato nella regolamentazione della materia, mediante l'introduzione, in particolare, del principio di *accountability*[12], teso a responsabilizzare i titolari del trattamento nelle loro attività di "manipolazione" di dati personali. Si sono fatti portavoce di tale modificato approccio i vari Garanti europei i quali hanno irrogato sanzioni amministrative pecuniarie per la violazione dell'art. 32 GDPR[13], il quale disciplina uno degli strumenti attuativi del predetto principio. Tale articolo prevede non obblighi generalizzati di adozione di misure "minime" di sicurezza (*ex* art. 33 codice *privacy ante*-riforma), bensì una valutazione, rimessa al titolare e al responsabile del trattamento, delle misure di sicurezza da effettuare caso per caso in rapporto ai rischi specificamente individuati: una valutazione non aprioristica, bensì plasmata alle concrete esigenze di tutela dello specifico trattamento.

Così, la *Commission nationale de l'informatique et des libertés* – CNIL, il Garante *Privacy* francese, ha comminato una delle sanzioni più alte del 2019 (50 milioni di euro) nei confronti di Google LLC; il Garante *privacy* rumeno (*Autoritatea Naţională de*

[12] V., ampiamente, *infra*, § 5.

[13] Rubricato *Sicurezza del trattamento* dispone quanto segue: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento 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: a) la pseudo-minimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. 2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'art. 40 o a un meccanismo di certificazione approvato di cui all'art. 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al § 1 del presente art. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

Supraveghere a Prelucrării Datelor cu Caracter Personal) ha irrogato una sanzione di 130 mila euro (equivalenti a 613.912 lei rumeni) a Unicredit Bank S.A.; il Garante per la protezione dei dati personali dello Stato di Baden – Württemberg (*Landesbeauftragte Für Den Datenshutz Und Die Informationsfreiheit* – LFDI) ha sanzionato un sito di *chat on line* al pagamento della somma di 20.000 euro; ancora, il *Comissão Nacional de Protecção de Dados* – CNPD, il Garante *privacy* portoghese, ha condannato una struttura ospedaliera al pagamento di 400 mila euro per aver permesso accessi non autorizzati alle cartelle cliniche dei pazienti[14].

Sono stati diversi i casi sottoposti all'attenzione dell'Autorità di controllo di casa nostra concernenti la violazione del principio di *accountability*: in alcuni casi[15] il Garante ha deciso di comminare, in alternativa alle sanzioni amministrative pecuniarie, le altre sanzioni previste dall'art. 58, § 2, GDPR[16].

[14] Un caso simile è stato sottoposto all'attenzione del Garante *privacy* italiano: Provv. Garante *privacy*, 23 gennaio 2020, n. 18, doc. web. n. 9269629, in *garante privacy.it*. La clemenza del provvedimento è evidente: la sanzione amministrativa pecuniaria inflitta ammonta a 30.000 euro.

[15] Tra gli altri, Provv. Garante *privacy*, 20 giugno 2019, n. 133, doc. web. n. 9124420, in *garante privacy.it*; Provv. Garante privacy, 18 aprile 2019, n. 96, doc. web. n. 9105201, *ivi*; Provv. Garante *privacy*, 19 luglio 2018, n. 427, doc. web. n. 9039945, *ivi*.

[16] Il § 2 dell'art. 58 dispone quanto segue: «[o]gni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli artt. 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'art. 17, § 2, e dell'art. 19; h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli artt. 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono piú soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'art. 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale».

Nel provvedimento n. 83 del 4 aprile 2019[17], il c.d. caso Rousseau, invece, il Garante *privacy* ha comminato la sanzione di 50 mila euro all'Associazione Rousseau per la mancanza di adeguate misure di sicurezza a protezione dei dati personali degli iscritti alla omonima piattaforma: gli obiettivi di tale piattaforma sono «la gestione del MoVimento 5 Stelle nelle sue varie componenti elettive (Parlamenti italiano ed europeo, Consigli regionali e comunali) e la partecipazione degli iscritti alla vita del MoVimento 5 Stelle attraverso, ad esempio, la scrittura di leggi e il voto per la scelta delle liste elettorali o per dirimere posizioni all'interno del MoVimento 5 Stelle»[18]. Il caso è particolarmente rilevante per le riflessioni che stimola sul principio di *accountability*, colonna portante della nuova disciplina in materia di protezione dei dati personali, nonché sull'*e-voting*: in altri termini e in buona sostanza in esso sono ben condensate le tematiche oggetto del presente approfondimento.

La sanzione, inflitta ancora nel periodo di tolleranza descritto nell'introduzione della presente trattazione, ha rappresentato il culmine di diverse indagini effettuate dal Garante a partire dall'autunno del 2017. Infatti, ad inizio agosto 2017 la piattaforma ha subito l'attacco da parte di un *hacker*, che ha diffuso sul *web* i dati personali di alcuni iscritti del MoVimento 5 Stelle, partito strettamente legato all'Associazione Rousseau e che utilizza proprio l'omonima piattaforma per condurre operazioni di voto *on line*. Nonostante tre provvedimenti del Garante, l'Associazione non ha comunque attivato adeguate misure di sicurezza, compiendo soltanto piccoli passi avanti in materia di protezione dei dati. Il Garante ha quindi inflitto la sanzione specificando che il «mancato, completo tracciamento degli accessi al *database* del sistema Rousseau e delle operazioni sullo stesso compiute […] configura la violazione di quel generale dovere di controllo sulla liceità dei trattamenti che grava sul titolare del trattamento e, in particolare, dell'obbligo di assicurare più adeguate garanzie di riservatezza agli iscritti alla piattaforma medesima; ciò sia in ragione delle dimensioni delle banche dati in questione, sia della tipologia di dati raccolti nonché delle funzionalità che le caratterizzano (tra cui, in particolare, il sistema di *e-voting* che deve essere

[17] In *garanteprivacy.it*.

[18] È quanto si legge nel sito *vote.rousseau.movimento5stelle.it*. Per una descrizione del funzionamento e delle caratteristiche della piattaforma v., tra gli altri, P. BECCHI, *Democrazia diretta, democrazia digitale e M5s*, in *Cib. dir.*, 2017, 2, p. 252 ss. Sul MoVimento 5 Stelle v. anche G. IORIO, *I profili civilistici dei partiti politici*, Napoli, 2018, p. 151 ss.

necessariamente assistito da idonei accorgimenti a tutela dei dati personali dei votanti). Ciò a maggior ragione tenendo conto che tali banche dati sono particolarmente esposte al rischio di attività di *hackeraggio* o comunque ad attacchi informatici, quali quelli verificatisi più volte, anche successivamente al *data breach* di agosto 2017». A ciò si unisce la circostanza che «le misure adottate, consistenti in procedure organizzative o comunque non basate su automatismi informatici, lasciando esposti i risultati delle votazioni (per un'ampia finestra temporale che si estende dall'istante di apertura delle urne fino alla successiva c.d. "certificazione" dei risultati, che può avvenire a distanza di diversi giorni dalla chiusura delle operazioni di voto) ad accessi ed elaborazioni di vario tipo (che vanno dalla mera consultazione a possibili alterazioni o soppressioni, all'estrazione di copie anche *offline*), non garantiscano l'adeguata protezione dei dati personali relativi alle votazioni *online* […]. La rilevata assenza di adeguate procedure di *auditing* informatico, escludendo la possibilità di verifica *ex post* delle attività compiute, non consente di garantire l'integrità, l'autenticità e la segretezza delle espressioni di voto, caratteristiche fondamentali di una piattaforma di *e-voting*». Si precisa, poi, che «l'accertata condivisione delle credenziali di autenticazione da parte di più incaricati dotati di elevati privilegi per la gestione della piattaforma Rousseau e la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività, nel previgente ordinamento erano addirittura qualificate come misure minime di sicurezza […] che i titolari del trattamento erano tenuti ad adottare al fine di assicurare un livello minimo di protezione dei dati personali. È pertanto evidente come la mancata adozione di tali misure e, per converso, l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresentino una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate»[19]. Le parole conclusive del Garante sono un chiaro richiamo al principio di *accountability*: «[s]olo in base ad una rigorosa progettazione e a una attenta valutazione dei rischi è, infatti, possibile realizzare un sistema di *e-voting* in

[19] V. Provv. Garante *privacy*, 10 gennaio 2019, n. 5, doc. web. n. 9080914, c.d. caso Cambridge Analytica, in *garanteprivacy.it*, caso nel quale l'Autorità di controllo si trova di fronte alla questione della "manipolazione" di dati politici.

grado di fornire garanzie di resilienza nonché di assicurare l'autenticità e la riservatezza delle espressioni di voto».

In buona sostanza ciò che è contestato alla piattaforma Rousseau è il ricorso a dispositivi e sistemi obsoleti nonché a misure tecniche e organizzative carenti nel trattamento di dati personali, dati che oltretutto si inseriscono nel novero dei dati particolari *ex* art. 9, § 1, GDPR[20]: misure che non consentono la protezione delle schede elettroniche, l'anonimato dei votanti in tutte le fasi del procedimento elettorale elettronico e la "non manomissione" dei voti.

Rilevante, anche e soprattutto per l'importo della sanzione, è il recentissimo caso Tim[21]. Il Garante per la *privacy* ha irrogato a Tim s.p.a. una sanzione di circa 27 milioni e 800 mila euro per numerosi trattamenti illeciti di dati legati all'attività di *marketing*. Le violazioni hanno interessato nel complesso alcuni milioni di persone e riguardano principalmente: chiamate promozionali indesiderate effettuate senza consenso, nonostante l'iscrizione delle utenze telefoniche nel Registro pubblico delle opposizioni oppure malgrado il fatto che le persone contattate avessero espresso alla società la volontà di non ricevere telefonate promozionali (chiamate effettuate da gennaio 2017 ai primi mesi del 2019); acquisizione obbligata del consenso a fini promozionali per poter aderire al programma "*Tim Party*" con i suoi sconti e premi; utilizzo di modulistica cartacea con richiesta di un unico consenso per diverse finalità, inclusa quella di *marketing*; gestione poco efficiente dei *data breach* e inadeguatezza dell'implementazione e della gestione dei sistemi che trattano dati personali, con violazione del principio di *privacy by design*.

In definitiva, le violazioni perpetrate da Tim s.p.a. denotano la totale mancanza di contezza di fondamentali aspetti dei trattamenti di dati effettuati, con particolare

[20] «1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

[21] Provv. Garante *privacy*, 15 gennaio 2020, n. 7, doc. web n. 9256486, in *garanteprivacy.it*. Tra i provvedimenti con i quali l'Autorità di controllo italiana infligge sanzioni pecuniarie per violazione del principio di *accountability* si vedano, tra i più recenti e tra gli altri, Provv. Garante *privacy*, 23 gennaio 2020, n. 18, doc. web. n. 9269629, cit.; Provv. Garante *privacy*, 23 gennaio 2020, n. 17, doc. web. 9269618, in *garante privacy.it*; Provv. Garante *privacy*, 11 dicembre 2019, n. 231, doc. web. n. 9244358, *ivi*.

riguardo al principio di *accountability*, ripetutamente oltraggiato dai comportamenti posti in essere dal colosso telefonico.

Oltre alla sanzione pecuniaria, l'Autorità ha imposto a Tim venti misure correttive, tra divieti e prescrizioni: il divieto dell'utilizzo dei dati a fini di *marketing* di chi aveva espresso ai *call center* il proprio diniego a ricevere telefonate promozionali, dei soggetti presenti in *black list* e dei "non clienti" che non avevano dato il consenso; il medesimo divieto è esteso ai dati della clientela raccolti mediante le app "*My Tim*", "*Tim Personal*" e "*Tim Smart Kid*" per finalità diverse dall'erogazione dei servizi senza un consenso libero e specifico; la verifica della consistenza delle *black lists* utilizzate; consentire l'accesso dei clienti a sconti e concorsi a premi eliminando il consenso obbligato al *marketing*; l'implementazione delle misure tecniche e organizzative relative alla gestione delle istanze di esercizio dei diritti degli interessati e rafforzamento delle misure volte ad assicurare la qualità, l'esattezza e il tempestivo aggiornamento dei dati personali trattati dai diversi sistemi della società.

*4. Le nuove tecnologie e l'***e-voting.**

Come si è anticipato, i casi analizzati – in particolare il caso Rousseau – aprono un interessante scenario sull'impatto dell'utilizzo delle nuove tecnologie sulla tutela della *privacy*.

La nostra è un'epoca contrassegnata dall'esplosione delle conoscenze e dall'incessante irruzione delle tecnologie avanzate: le tecnologie dell'informazione e della comunicazione, intese come la convergenza di informatica e telematica per nuovi modi di gestire e comunicare l'informazione – includenti internet, l'architettura aperta di rete, la multimedialità – hanno notevolmente inciso sulla scienza giuridica[22].

[22] La bibliografia sul tema è molto ampia: si richiamano, tra gli altri, R. BORRUSO, Computer *e diritto*, I, II, Milano, 1985; G. CORASANITI, *Diritto e tecnologie dell'informazione*, Milano, 1990; P. ZANELLI, *Nuove tecnologie*, Milano, 1993; V. RIZZO, *Diritto e tecnologie dell'informazione*, Napoli, 1998; I. D'ELIA CIAMPI, *Diritto e nuove tecnologie dell'informazione*, Napoli, 1998; G. CIACCI, P. DI SALVATORE, P. GALDIERI e M. MINERVA, *Prospettive giuridiche delle tecnologie dell'informazione*, Napoli, 2000; G. CASSANO (a cura di), *Internet. Nuovi problemi e questioni controverse*, Milano, 2001; R. NANNUCCI (a cura di), *Lineamenti di informatica giuridica*, Napoli, 2002; G. ZICCARDI (a cura di), *Crittografia e diritto*, Torino, 2003; G. BISCONTINI-L. RUGGERI (a cura di), *Diritti del cittadino e tecnologie informatiche*, Napoli, 2004; A. DI AMATO, *Appunti di diritto dei mezzi di comunicazione*, Napoli, 2006; M. CUNIBERTI, *Nuove tecnologie e libertà della comunicazione. Profili costituzionali e pubblicistici*, Milano, 2008; G. CASSANO, *Diritto dell'Internet*

Tale nuovo scenario tecnologico, il cui principale punto di svolta è ovviamente rappresentato da internet, «pone il giurista di fronte a questioni nuove e diverse e, talvolta, a sfide intellettuali che ne mettono in discussione la capacità di mediare tra l'astrattezza della norma giuridica e la concretezza dei problemi originati dall'evoluzione socio-economica»[23].

La tecnologia digitale, in particolare internet, costituisce un'innovazione che non vive per conto proprio in una realtà virtuale, ma incide notevolmente su quella effettiva, stimolando a cambiare i rapporti umani ed economici e lo stesso modo di intendere il sistema ordinamentale[24]. Esso ha inciso sensibilmente sui rapporti socio-economici e su quelli civili, rivoluzionando e sconvolgendo abitudini di vita radicate nella società civile e ha fortemente condizionato le relazioni dell'uomo in un ambiente privo di confini, lo spazio c.d. cibernetico, che, attesa la sua virtualità, comporta non un movimento fisico di cose, bensì un movimento di impulsi elettronici[25].

A internet vanno attribuiti il merito di aver prodotto innumerevoli benefici e la responsabilità di aver dato vita a numerosi svantaggi: quanto ai primi, ha facilitato i rapporti a distanza consentendo di negoziare, creare documenti elettronici validi e rilevanti ai fini della prova, di immetterli nel traffico dello spazio cibernetico delle reti telematiche di trasmissione, ha determinato lo sviluppo dell'*e-commerce*, ha permesso nuove modalità di dialogo tra il mercato e la persona e messo in relazione due o più soggetti tra loro distanti[26]. Quanto alle ripercussioni negative è sufficiente rilevare che «nella sua aspirazione alla pervasività globale, è minato da *deficit* economici, culturali e di sviluppo dei singoli Paesi per via di nuove forme di diseguaglianze, dovute alla

---

e delle nuove tecnologie telematiche, Padova, 2009; S. FARO-N. LETTIERI-A. TARTAGLIA POLCINI (a cura di), *Diritto e tecnologie. Verso le scienze computazionali. Attualità e orizzonti dell'Informatica giuridica*, Napoli, 2012; M. JORI, *Diritto, nuove tecnologie e comunicazione digitale*, Milano, 2013; C. PERLINGIERI-L. RUGGERI (a cura di), *Internet e diritto civile*, Napoli, 2015.

[23] G. PERLINGIERI, *Il contratto telematico*, in D. VALENTINO (a cura di), *Manuale di diritto dell'informatica*, Napoli, 2004, p. 266.

[24] P. PERLINGIERI, *Relazione conclusiva*, in C. PERLINGIERI-L. RUGGERI (a cura di), *Internet e diritto civile*, cit., p. 417.

[25] C. PERLINGIERI, *Presentazione*, in C. PERLINGIERI-L. RUGGERI (a cura di), *Internet e diritto civile*, cit., p. 5. «Con Internet è avvenuta una rivoluzione nel sistema della comunicazione paragonabile all'invenzione della stampa a caratteri mobili nel XV secolo»: queste le parole di P. BECCHI, *Democrazia diretta, democrazia digitale e M5s*, cit., p. 244.

[26] G. PERLINGIERI, *Il contratto telematico*, cit., p. 270 ss.

carenza, a volte, di strutture informatiche e telematiche, altre volte, di conoscenza e formazione dei suoi potenziali fruitori»[27].

Per ciò che rileva in questa sede, si può affermare che l'evoluzione tecnologica e la diffusione dei contenuti digitali in Rete rappresentano fattori di immenso cambiamento per la tutela della persona e del mercato. In ogni momento una enorme quantità di dati personali vengono, anche a nostra insaputa, raccolti, conservati e trattati dagli operatori della Rete, creando un flusso in costante movimento, sempre più fuori controllo da parte dei soggetti interessati; ad un tempo, la vita delle persone è sempre più orientata a svolgersi nello spazio digitale, dove si concentrano interessi lavorativi, personali, familiari e relazionali, lasciando nel Web, ad ogni passaggio, informazioni personali, tracce di sé[28]. Conseguenza inevitabile di tale diffusa prassi è che la sfera privata degli individui si assottiglia e diventa sempre più fragile[29].

Il caso Rousseau è paradigmatico delle negative conseguenze causate dall'inesorabile avanzare delle nuove tecnologie sulla *privacy*: nello specifico, esso solletica la riflessione sulla interazione tra il voto elettronico e la tutela della riservatezza.

Fondamentale è avere contezza dei termini adoperati: con l'espressione voto elettronico si vuole indicare una manifestazione della *e-democracy*[30], «il processo ed il

---

[27] P. PERLINGIERI, *Relazione conclusiva*, cit., 418 s., e *ivi* ulteriori approfondimenti. Sui rischi della connettività v. anche G. ROMANO, *L'attuazione delle obbligazioni in rete*, in C. PERLINGIERI-L. RUGGERI (a cura di), *Internet e diritto civile*, cit., p. 391, nota 21.

[28] Quasi testualmente, P. PERLINGIERI, Privacy d*igitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, 2, p. 481.

[29] P. PERLINGIERI, *o.l.u.c.*

[30] Sulla democrazia digitale v., tra gli altri, i seguenti scritti: A. DI GIOVINE, *Democrazia elettronica: alcune riflessioni*, in *Dir. soc.*, 1995, p. 399 ss.; E. BETTINELLI, *La lunga marcia del voto elettronico in Italia*, in *Quad. Osserv. elettorale*, 2002, 46, p. 15 ss.; G. OROFINO, *L'*e-vote, in F. SARZANA DI S. IPPOLITO (a cura di), E-government: *profili teorici ed applicazioni pratiche del governo digitale*, Piacenza, 2003, p. 363 ss.; P. COSTANZO, *La democrazia elettronica (note minime sulla c.d.* e-democracy), in *Dir. inf.*, 2003, p. 465 ss.; T.E. FROSINI, *Tecnologie e libertà costituzionali*, *ivi*, 2003, p. 487 ss.; S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2004; F. DI MASCIO, *Democrazia elettronica: insidie, illusioni, prospettive*, in *Cib. dir.*, 2005, 3, p. 317 ss.; A. GRATTERI, *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, Padova, 2005; R.M. DI GIORGI, *Lo Stato essenziale. Semplicità, cultura e democrazia al tempo della rete*, Napoli, 2006; G. OROFINO, *L'espressione elettronica del suffragio*, in *Dir. internet*, 2006, 2, p. 201 ss.; A. SARAIS, *Democrazia e tecnologie. Il voto elettronico*, Bologna, 2008; M. CUNIBERTI (a cura di), *Nuove tecnologie e libertà della comunicazione. Aspetti costituzionali e pubblicistici*, Milano, 2008; F. PIZZETTI, *Partiti politici e nuove tecnologie*, in *federalismi.it*, 2008, n. 21; F. AMORETTI ed E. GARGIULO, *Dall'appartenenza materiale*

risultato dell'applicazione alle operazioni elettorali delle nuove tecnologie informatiche»[31]. Volendo entrare più nel dettaglio l'*e-voting* «raggruppa approcci ben distinti che spaziano dall'uso di sistemi per la lettura ottica della scheda cartacea, alle macchine per voto assistito con registrazione diretta (*direct-recording eletronic*-DRE), fino al voto elettronico su rete pubblica (utilizzando l'Internet mondiale)»[32].

Senza alcuna pretesa di completezza, pare dovuto il rimando alla questione, diffusamente approfondita in dottrina, del rapporto tra il voto elettronico e la Costituzione italiana: i dubbi concernono l'idoneità dell'*e-voting* a salvaguardare le garanzie di cui all'art. 48 cost: personalità, eguaglianza, libertà e segretezza del voto.

Premesso che falle nell'assicurare i princípi di cui al citato articolo sono rinvenibili anche nel sistema elettorale tradizionale fondato sull'utilizzo della scheda cartacea, la dottrina ha sottolineato la presenza di numerosi limiti dell'*e-voting* nell'assicurare le guarentigie previste dai Padri costituenti. Così, secondo alcuni[33], il requisito della personalità del voto non risulterebbe pienamente soddisfatto dalle moderne tecniche di identificazione a distanza, le quali, se pur potenzialmente idonee a garantire la

---

all'appartenenza virtuale? La cittadinanza elettronica fra processi di costituzionalizzazione della rete e dinamiche di esclusione, in *Pol. dir.*, 2010, p. 353 ss.; M. ROSPI, *Internet e diritto di voto*, in M. NISTICÒ e P. PASSAGLIA, *Internet e Costituzione*, Torino, 2014, p. 263 ss.; P. CARLOTTO, *Il voto elettronico nelle democrazie contemporanee*, Padova, 2015; M. CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Dir. inf.*, 2015, 2, p. 275 ss.; A. GRATTIERI, *Finalità e problemi del voto elettronico: le prospettive della sua attuazione in Italia*, in *Forum Quad. cost.*, *Rassegna*, 25 marzo 2015; L. TRUCCO, *Il voto elettronico nel quadro della democrazia digitale*, in T.E. FROSINI, O. POLLICINO, E. APA e M. BESSINI (a cura di), *Diritti e libertà in Internet*, Milano, 2017; T.E. FROSINI, *Internet e democrazia*, in *Dir. inf.*, 4-5, 2017, p. 657 ss.; G. PEPE, *Democrazia rappresentativa e democrazia partecipativa nell'età della rivoluzione informatica*, in *Comparazione e diritto civile*, 2019, 1, p. 323 ss. Per un'analisi degli aspetti comparatistici si v., tra i tanti contributi, L. CUOCOLO, *Voto elettronico e post-democrazia nel diritto costituzionale comparato*, in *Dir. pubbl. comp. eur.*, 2002, p. 255 ss.; L. TRUCCO, *Il voto elettronico nella prospettiva italiana e comparata*, in *Dir. inf.*, 2011, p. 47 ss.

[31] A. SARAIS, *Democrazia e tecnologie. Il voto elettronico*, cit., p. 20 s.

[32] A. BERNI, E-voting: *il punto della situazione*, in *internetvoting.it*. Le nuove tecnologie incidono anche sui sistemi di voto nelle assemblee societarie: per una disamina delle caratteristiche e dei principali problemi emergenti si v., per tutti, M. CIAN, *L'intervento e il voto elettronico nelle assemblee di s.p.a.*, in *Riv. soc.*, 2011, p. 1065 ss.; ID., *Intervento e voto in assemblea: le nuove tecnologie come mezzo per promuovere l'attivismo degli investitori istituzionali?*, in *Banca borsa tit. cred.*, 2014, p. 420 ss.; G.P. LA SALA, *Le forme di partecipazione assembleare con mezzi elettronici nella società per azioni*, *ivi*, 2016, p. 690 ss.

[33] G. OROFINO, *L'*e-vote, cit., *passim*. Sulla necessità di attivare una serie di accorgimenti tecnici finalizzati a consentire un'identificazione sicura e univoca dell'elettore che gli consentano di votare una sola volta, disattivandosi automaticamente nell'ipotesi in cui si volesse esprimere fraudolentemente un voto plurimo v. A. SARAIS, *Democrazia e tecnologie. Il voto elettronico*, cit., p. 57. Sulla questione v. anche M. ROSPI, *Internet e diritto di voto*, cit., p. 268.

personalità del votante al momento dell'identificazione, non appaiono utili ad assicurare che, subito dopo il riconoscimento, l'avente diritto al voto lasci votare in sua vece altra persona: in altri termini non è garantita l'identità tra chi trasmette il voto e il titolare del diritto elettorale (si pensi anche all'ipotesi di un terzo che in modo fraudolento si appropri della *password* dell'elettore). Problemi soltanto in parte superabili ricorrendo alle moderne tecniche di identificazione attraverso i dati biometrici dell'elettore[34].

Ulteriori dubbi riguardano poi la segretezza del voto, principio strettamente funzionale a quello della libertà dello stesso: si è condivisibilmente rilevato che, per quanto si possano adottare i più raffinati strumenti offerti dalla tecnologia, non si vede come si possa scongiurare la possibilità che l'elettore, nel momento nel quale esprime il proprio voto da un terminale collocato fuori dal seggio elettorale, sia esposto allo sguardo di altri, in grado di prendere conoscenza del suo voto e quindi di condizionarlo[35].

Problematiche aggiuntive legate all'uso della tecnologia nei sistemi di votazione attengono alla sicurezza informatica del procedimento per quanto riguarda sia il *software* sia l'*hardware* utilizzati: devono essere infatti esclusi rischi di sorta in relazione a possibili malfunzionamenti o manipolazioni del voto insite negli apparati utilizzati così come non può essere sottovalutato il possibile attacco di *hacker* intenzionati a realizzare un broglio[36]. Ne discende, in particolare, l'esigenza di adottare programmi *software* dotati di codici sorgente *open source* al fine di rendere effettivo il controllo pubblico e non di programmi con codici sorgente proprietari[37].

---

[34] Cfr. M. CUNIBERTI, *Nuove tecnologie e libertà politiche*, cit., p. 275 ss.

[35] M. CUNIBERTI, *o.l.u.c.*, il quale differenzia, graduandone le problematiche collegate, il caso del voto attraverso terminali collocati nei seggi elettorali – per il quale il pericolo di manipolazioni non pare molto diverso da quello che si può porre in presenza del voto cartaceo – e il c.d. *home vote* che pone, come visto nel testo, problemi costituzionali ben piú gravi. Sostiene, partendo da un parallelismo con i *social networks*, che l'*e-democracy* non metta a rischio la segretezza del voto T.E. FROSINI, *Internet e democrazia*, cit., p. 657 ss. V. già ID., *Tecnologie e libertà costituzionali*, cit., p. 487 ss. Sulla questione della segretezza v. anche E. BETTINELLI, *La lunga marcia del voto elettronico in Italia*, cit., p. 15; A. GRATTERI, *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, cit., p. 86 ss.; G. OROFINO, *L'espressione elettronica del suffragio*, cit., p. 203 ss.

[36] Quasi testualmente A. GRATTIERI, *Finalità e problemi del voto elettronico: le prospettive della sua attuazione in Italia*, cit.,

[37] Quasi testualmente A. GRATTIERI, *o.u.c.*, ed *ivi* una rassegna di pronunce giurisprudenziali che hanno segnato una battuta d'arresto del voto elettronico in vari Paesi europei. Sulle

A tal ultimo proposito, si è rilevato, già prima dell'intervento del Garante *privacy*, che la piattaforma Rousseau non amplia la democrazia ma la restringe. Ciò è dovuto principalmente alla circostanza che il "sistema operativo" della piattaforma è a codice chiuso, cioè segreto: nessuno, tranne i suoi programmatori, può conoscerne il funzionamento e ciò non permette la verificabilità e la tracciabilità di quanto avviene all'interno del sistema[38]. Di conseguenza, «ci si deve fidare» dell'operato dei programmatori[39]. Tutto ciò, come già accennato relativamente ai principali problemi del voto elettronico, è fortemente rischioso per la democrazia: manipolare e alterare i risultati senza che il sistema se ne accorga (e neppure gli elettori) è operazione molto semplice in tali meccanismi chiusi. A ciò si aggiunga la circostanza che il numero di iscritti alla piattaforma Rousseau rimane, ad oggi, un mistero.

Il Garante, con il provvedimento oggetto di esame, aggiunge un tassello ulteriore al quadro già particolarmente spinoso emerso dalle riflessioni compiute: alle insidie che si annidano nel sistema di voto elettronico e ai *deficit* strutturali della piattaforma Rousseau si sommano le falle nel sistema di sicurezza della stessa, le quali, tradendo le garanzie costituzionali dell'autenticità, dell'integrità e della segretezza del voto, non assicurano un'adeguata protezione dei dati personali relativi alle votazioni *on line*. È questo un chiaro esempio di interazione negativa tra il modello evoluto di votare e la tutela della *privacy*.

In definitiva, i problemi della piattaforma sono di due tipi: uno, per così dire, strutturale, legato al tipo di "sistema operativo" adoperato e, come chiarito dal

---

modalità di espressione di voto nei Paesi membri dell'Unione Europea e sulla interazione tra il voto elettronico e i princípi costituzionali v., già, ID., *Il valore del voto. Nuove tecnologie e partecipazione elettorale*, cit., *passim*.

[38] P. BECCHI, *Democrazia diretta, democrazia digitale e M5s*, cit., pp. 254 e 256, il quale aggiunge che «[q]uesta è la prima, essenziale differenza tra *Liquid Feedback* e "piattaforma Rousseau." Nel primo, il software (ossia quell'insieme d'istruzioni scritte da programmatori che permettono al computer di effettuare operazioni) è libero, visibile e disponibile per tutti. Nel secondo, no. Come sanno tutti gli esperti, il passaggio dal software chiuso (o "proprietario") a quello "aperto" è stato un momento essenziale nel mondo dell'informatica, soprattutto in un'ottica di libertà, sicurezza e democrazia». L'a. conclude affermando che la democrazia della piattaforma Rousseau «non è né democrazia rappresentativa, né democrazia diretta, né democrazia digitale: è la negazione tout-court della democrazia».

[39] Aggiunge P. BECCHI, *Democrazia diretta, democrazia digitale e M5s*, cit., p. 255: «esattamente come ha scritto Grillo di recente: "fidatevi di me"». Dubitativo sulla idoneità dei "meccanismi" adoperati all'interno del Movimento 5 Stelle di garantire effettive *chances* di partecipazione democratica anche F. PIZZETTI, *Partiti politici e nuove tecnologie*, cit.

Garante, all'obsolescenza di alcune componenti *software* dei siti *web* del Movimento e l'altro "procedurale", il quale si concretizza nella violazione delle misure di sicurezza idonee a garantire la democraticità delle votazioni *on line*. Riflessioni queste che conducono senza esitazione alcuna e, lo si consenta, al netto dei vari "scandali politici" legati alla piattaforma Rousseau, ad accogliere con favore la decisione dell'Autorità di controllo italiana.

Le significative parole di Giovanni Buttarelli, pronunciate a margine della presentazione a Bruxelles del Rapporto annuale del 2018 sulla protezione dei dati personali[40], paiono racchiudere il senso di quanto si è detto sinora: l'*ex* Garante europeo della *privacy*, manifestando, a ragion veduta, perplessità riguardo alla piattaforma Rousseau e definendola al contempo un esempio della necessaria evoluzione della politica, afferma che la democrazia elettronica non è soltanto quella di un partito politico, ma può aprire opportunità anche per i Comuni e le Regioni per le consultazioni pubbliche, ferme restando la necessità di intervenire sulle falle della sicurezza *on line* e l'assunzione dei dati personali a pilastro essenziale della democrazia. Dunque «non è la democrazia che deve diventare elettronica quanto l'elettronica che deve diventare democratica»[41].

5. Il principio di accountability.

Le parole dell'*ex* Garante europeo si rivelano preziose anche per spiegare in maniera chiara ed essenziale il più volte richiamato principio di *accountability*[42], protagonista

---

[40] V. *edps.europa.eu.it*.

[41] P. COSTANZO, *La democrazia elettronica (note minime sulla cd.* e-democracy), cit., p. 492. Sulla necessità della democraticità del voto elettronico v., per tutti, P. CARLOTTO, *Il voto elettronico nelle democrazie contemporanee*, cit., *passim*.

[42] Per i riferimenti normativi del principio di responsabilizzazione v. i considerando nn. 74, 75, 78 e 85, gli artt. 23-25 e l'intero Capo IV, reg. UE n. 679 del 2016. In dottrina, tra gli altri, oltre ai contributi citati *supra* nella nota 2, M. D'AMBROSIO, *Progresso tecnologico, «responsabilizzazione» dell'impresa ed educazione dell'utente*, Napoli, 2017, *passim*, ma spec. p. 123 ss., il quale, concentrandosi soprattutto sulla responsabilizzazione dell'impresa fornitrice di servizi informatici, definisce l'*accountability* quale insieme di doveri protesi ad assicurare un sufficiente rapporto di fiducia con i destinatari dei servizi; R. CELELLA, *Il principio di responsabilizzazione: la novità del GDPR*, in *Cib. dir.*, 2018, 1-2, p. 211 ss.; G. RUSSO e M. POLINI, *I principi di* accountability *e di effettività nel nuovo regolamento*, in M. MAGLIO, M. POLLINI e N. TILLI, *Manuale di diritto alla protezione dei dati personali. La* privacy *dopo il Regolamento UE 2016/679*, cit., p. 127 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori. Commento a Reg. UE 2016/679*, in *Contr. impr.*, 2018, 1, p. 106 ss.; F.

assoluto della riforma in materia di protezione dei dati personali: «[a]i titolari del trattamento nel settore pubblico e privato sarà richiesto non semplicemente di rispettare le norme, e quindi di fare una *check-list* degli adempimenti minimi, ma di tradurre in pratica questi princípi con diversi "compiti a casa" in chiave di creatività e proattività. Dovranno dimostrare di aver distribuito responsabilità al proprio interno, di avere una risposta per i vari problemi, di aver valutato i rischi e le possibili conseguenze, e quindi di avere una strategia articolata e trasparente nei confronti dei soggetti cui si riferiscono le informazioni. Non sarà più una materia delegabile a un funzionario di turno, a un esperto di tecnologia o a un ufficio legale; sarà proprio l'approccio corporeo che avrà importanza, anche perché si dovranno individuare anche linee di bilancio importanti»[43].

Dunque, tale principio responsabilizza i titolari del trattamento, i quali dovranno adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento[44]. La nuova disciplina ha altresì predisposto una serie di strumenti utilizzabili dai titolari al fine di dimostrare l'osservanza delle prescrizioni imposte al titolare del trattamento e di adempiere all'onere di prova richiesto dal principio di responsabilizzazione.

Così, secondo l'art. 24 reg. l'adesione ai codici di condotta[45] o a un meccanismo di certificazione[46] può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento: tale adesione può, inoltre, assicurare la trasparenza del trattamento, con conseguente incremento della fiducia degli interessati che, grazie alla certificazione, possono valutare rapidamente il livello di protezione dei loro dati.

MAZZONI, *Regolamento Europeo 2016/679: alcune normazioni di riferimento per declinare sul campo il principio dell"*accountability*"*, in *Cib. dir.*, 2019, 1-2, p. 197 ss.

[43] Intervista a cura di Antonello Salerno: «*Tanti compiti a casa per gli Stati e l'Ue*», in *corrierecomunicazioni.it*, 2017.

[44] V. artt. 5 e 24 reg. n. 679 del 2016.

[45] Art. 40 reg. n. 679 del 2016.

[46] Artt. 42 e 43 reg. n. 679 del 2016. La certificazione può essere definita come l'atto mediante il quale una terza parte indipendente dichiara che, con ragionevole attendibilità, un determinato prodotto, processo o servizio è conforme a requisiti specificati. Le certificazioni sono rilasciate dagli organismi accreditati ai sensi delle norme ISO/IEC 17021-1 per i sistemi di gestione, ISO/IEC 17065 per i prodotti e servizi, ISO/IEC 17024 per le persone.

L'art. 25 reg.[47] disciplina gli strumenti della c.d. protezione fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*). Essi suppliscono, rispettivamente, alla necessità di configurare il trattamento prevedendo fin dall'inizio, mediante un'analisi preventiva da attuare già prima di procedere al trattamento, le garanzie indispensabili al fine di attuare in modo efficace i princípi di protezione dei dati del regolamento – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati – e quella di trattare soltanto i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini[48]. Le tecniche del *privacy by design*, *privacy by default* e *accountability privacy* sono state opportunamente definite quale adeguato strumentario messo in campo al fine di riequilibrare il rapporto tra operatore

[47] Rubricato *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* statuisce quanto segue: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'àmbito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudo-minimizzazione, volte ad attuare in modo efficace i princípi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. 2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica. 3. Un meccanismo di certificazione approvato ai sensi dell'art. 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai §§ 1 e 2 del presente articolo».

[48] Per un'analisi degli strumenti citati nel testo, in particolare delle loro criticità e dei metodi per la loro applicazione, v. E. ERRICHIELLO, Privacy by design *e* privacy by default*: origini, prospettive e criticità*, in *Data Protection Law*, 2018, 1, p. 3 ss. Sul tema anche G. D'ACQUISTO e M. NALDI, Big data *e* privacy by design, Torino, 2017; A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, in *Contr. impr./Eur.*, 2015, p. 197 ss. Tra i provvedimenti che l'Autorità di controllo italiana ha emanato facendo leva sui princípi descritti nel testo si v., tra gli altri, Provv. Garante *privacy*, 23 gennaio 2020, n. 18, doc. web. n. 9269629, cit.; Provv. Garante *privacy*, 18 aprile 2019, n. 96, doc. web. n. 9105201, cit.; Provv. Garante *privacy*, 19 luglio 2018, n. 427, doc. web. n. 9039945, cit.; Provv. Garante *privacy*, 28 giugno 2018, n. 396, con nota di N. MINISCALCO, *Uno, nessuno o centomila? Minimizzazione e* privacy by default *nel primo provvedimento del Garante dopo il GDPR*, in *Dir. inf.*, 2018, p. 782 ss.

informatico e utente, di realizzare in maniera efficace i princípi di protezione dei dati e di porre l'utente al centro dell'attività informatica[49].

La nuova disciplina introduce un particolare strumento teso a gestire i rischi insiti nel trattamento dei dati e a prevenirli: la valutazione di impatto sulla protezione dei dati personali – DPIA, *Data Privacy Impact Assessment*[50]. Di essa il regolamento non fornisce una definizione: le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679», adottate dal Gruppo di lavoro Articolo 29[51], lo definiscono come «un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli», precisando che essa concretizza uno strumento importante per la responsabilizzazione perché sostiene «i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento».

Lungi dall'esaminare nel dettaglio il funzionamento di tale strumento, per il quale si rinvia ai particolareggiati artt. 35 e 36 reg.[52], è opportuno in questa sede evidenziarne i

---

[49] Cosí M. D'AMBROSIO, *Progresso tecnologico, «responsabilizzazione» dell'impresa ed educazione dell'utente*, cit., pp. 23 ss. e 132 ss.

[50] Sulla questione v., per tutti, P. LA FARCIOLA, Data protection impact assessment *e sicurezza dei dati. Novità e criticità alla luce del principio di* accountability *nel Regolamento UE per la protezione dati personali 679/2016*, in *Data Protection Law*, 2020, 1, p. 3 ss. Qualche brevissima riflessione anche in M.G. STANZIONE, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, cit., p. 1249 ss.

[51] In *ec.europa.eu*.

[52] Secondo l'art. 35 rubricato *Valutazione d'impatto sulla protezione dei dati* «1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. 2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno. 3. La valutazione d'impatto sulla protezione dei dati di cui al § 1 è richiesta in particolare nei casi seguenti: a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie

particolari di dati personali di cui all'art. 9, § 1, o di dati relativi a condanne penali e a reati di cui all'art. 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. 4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del § 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'art. 68. 5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipolo-gie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato. 6. Prima di adottare gli elenchi di cui ai §§ 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'art. 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in piú Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. 7. La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al § 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione. 8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'art. 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati. 9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti. 10. Qualora il trattamento effettuato ai sensi dell'art. 6, § 1, lett. *c* o *e*, trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del tratta-mento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'àmbito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i §§ da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento. 11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento».

Il seguente art. 36 rubricato *Consultazione preventiva* dispone che «1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'art. 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. 2. Se ritiene che il trattamento previsto di cui al § 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'art. 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione. 3. Al momento di consultare l'autorità di controllo ai sensi del § 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare

punti di forza: identificazione e gestione dei rischi; prevenzione della possibilità che determinati problemi vengano scoperti in uno stadio avanzato del trattamento; gestione tempestiva dei rischi connessi al trattamento con conseguente possibilità di introdurre preventivamente appropriate misure di controllo; rafforzamento del livello di affidabilità legato all'immagine dell'azienda. Per comprendere compiutamente la portata della novità introdotta giova segnalare un passaggio di rilievo avvenuto con la nuova normativa: il passaggio dal DPS, documento programmatico sulla sicurezza, un adempimento formale, una fotografia documentata dell'adeguatezza delle misure di sicurezza adottate per trattare i dati personali, alla DPIA, che può sinteticamente essere definita quale analisi profonda dei processi aziendali e dei rischi in concreto generati dal trattamento dei dati, al fine di gestirli al meglio e prevenirli.

Ulteriori misure di sicurezza atte a dare attuazione al principio in esame sono – oltre a quelle contenute nel più volte citato e vilipeso art. 32 – il Registro dei trattamenti[53], il quale risponde alla duplice esigenza di adottare misure di responsabilizzazione per il titolare e il responsabile del trattamento e di permettere la successiva verifica da parte dell'Autorità di controllo del rispetto della normativa da parte dei soggetti obbligati[54], nonché il *data breach notification*[55], ossia la notificazione delle violazioni dei dati personali suscettibili di presentare un rischio elevato per i diritti e le libertà degli interessati: in tal modo si fornisce alle Autorità di controllo un valido strumento per consentire loro di attivarsi prontamente in modo da valutare la gravità della violazione e le misure da imporre al titolare.

---

relativamente al trattamento nell'àmbito di un gruppo imprenditoriale; b) le finalità e i mezzi del trattamento previsto; c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; d) ove applicabile, i dati di contatto del titolare della protezione dei dati; e) la valutazione d'impatto sulla protezione dei dati di cui all'art. 35; f) ogni altra informazione richiesta dall'autorità di controllo. 4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento. 5. Nonostante il § 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica».

[53] Si rinvia all'art. 30 reg. n. 679 del 2016.

[54] GEA ARCELLA, *GDPR: il Registro delle attività di trattamento e le misure di "*accountability*"*, in *Notariato*, 2018, 4, p. 393 ss.

[55] Disciplinato agli artt. 33 e 34 reg. n. 679 del 2016.

Allo scopo di responsabilizzare i titolari e i responsabili del trattamento sono stati posti obblighi di trasparenza più stringenti[56]: in particolare, in tema di informativa[57] si è passati da una situazione nella quale non vi erano peculiari requisiti per la sua stesura – l'informativa era spesso lunga, incomprensibile e con richiami normativi complessi – al contesto attuale ove i titolari e i responsabili del trattamento sono tenuti a predisporre una informativa accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi. Numerose e rilevanti modifiche orientate alla trasparenza hanno interessato anche il consenso[58]: in estrema sintesi si può seraficamente asserire che il regolamento europeo si concreta, più che sui requisiti formali del consenso, sulla necessità della validità sostanziale dello stesso, per far sì che l'interessato sia pienamente consapevole e informato quando lo presta[59].

A questo punto un richiamo merita la questione delle lesioni dei diritti della personalità e degli strumenti che l'ordinamento predispone per farvi fronte. È intuitivo che la riparazione dei danni in materia di diritti della personalità si pone in termini alquanto diversi rispetto ad altre situazioni soggettive, dal momento che la lesione subíta non è suscettibile di essere reintegrata in forma specifica mediante il ripristino della situazione antecedente alla lesione: anche quando il danno subíto può essere risarcito pecuniariamente, si ha non ristoro della situazione precedente, ma semplicemente un equivalente in termini monetari. È altrettanto evidente l'insufficienza della tutela successiva alla lesione – che è pur sempre di contenuto economico – soprattutto per quegli aspetti maggiormente qualificanti la natura dei diritti della personalità che non hanno un contenuto economico. In una più idonea prospettiva di prevenzione del danno, o almeno di sua tempestiva cessazione, si

[56] Si v. i considerando 13, 39, 58, 78 e 100, l'art. 5 nonché la Sezione 1 del Capo III in tema di Diritti dell'interessato. Sulla tematica della trasparenza v., tra gli altri e diffusamente, G. RUSSO e M. POLINI, *I principi di* accountability *e di effettività nel nuovo regolamento*, cit., p. 133 ss.

[57] Artt. 12, 13 e 14 reg. n. 679 del 2016.

[58] Artt. 4 e 7 reg. n. 679 del 2016.

[59] Sul consenso, sia con specifico riferimento alla tutela della *privacy* e alle nuove tecnologie sia con riferimento al tema particolarmente dibattuto della negoziabilità dei dati personali v., tra gli altri, C. PERLINGIERI, *Gli accordi tra i siti di* social networks *e gli utenti*, in *Rass. dir. civ.*, 2015, p. 104 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017; G. RESTA e Z. ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim.*, 2018, p. 411 ss.; L. TAFARO, Neuromarketing *e tutela del consenso*, Napoli, 2018; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, in *Quad. Foro nap.*, Napoli, 2019.

muovono altri criteri, già enunciati in relazione a singole ipotesi, anche se comuni a ogni altra fattispecie: l'inibitoria, ad esempio, che è diretta a far cessare (o a non far iniziare) il comportamento antigiuridico del danneggiante (7, 9, 10 c.c.), o altro rimedio di urgenza (700 c.p.c.), che può essere chiesto da chi ha fondato motivo di temere che, nel tempo necessario a far valere un suo diritto in via ordinaria, questo sia minacciato da pregiudizio imminente e irreparabile. L'introduzione sistematica o in via generale di tecniche di controllo sociale o la comminatoria di pene pecuniarie progressive in ragione del ritardo nella rimozione delle cause del danno, in via preventiva e il rafforzamento del sistema di sicurezza sociale, magari mediante la costituzione di un fondo di solidarietà con le pene private inflitte ai danneggianti, in via successiva, rappresentano le proposte *de iure condendo* della piú moderna dottrina[60].

La motivazione che ha indotto a richiamare, seppur fugacemente, tale problematica è lampante: il principio di *accountability* si incastra perfettamente in quella prospettiva di prevenzione del danno che, secondo la condivisibile ricostruzione appena esposta, sarebbe la piú idonea a tutelare adeguatamente i diritti della personalità. Il principio di *accountability* è espressione del passaggio da un approccio essenzialmente riparatorio – rivelatosi inadeguato – posto al centro della dir. 95/46/CE, a uno preventivo, che anticipa la tutela a un momento anteriore al trattamento dei dati personali e – mediante una visione che potremmo definire rischio-centrica[61], l'implementazione di una serie di misure di sicurezza, l'introduzione di una serie di obblighi posti a carico di chi maneggia i nostri dati personali – prevede un impegno attivo dei titolari fin dalla progettazione dei prodotti e servizi il cui utilizzo incida sui dati degli utenti[62] . Un po' come dire che anche quando si manipolano dati personali val la massima per la quale

[60] La ricostruzione riportata nel testo è di P. PERLINGIERI e L. LONARDO, *Lesioni alla personalità e strumenti di tutela*, in P. PERLINGIERI, *Manuale di diritto civile*, Napoli, 2018, p. 217.

[61] Sul punto v. A. MANTELERO, *Responsabilità e rischio nel Regolamento UE n. 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 147 ss. Per la definizione di rischio v. il considerando n. 75 del reg. UE n. 679 del 2016. Le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679» adottate dal Gruppo di lavoro Articolo 29, fanno riferimento al rischio inteso come «uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità, e la gestione del rischio è *ivi* definibile «come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio».

[62] M.G. STANZIONE, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, cit., p. 1249 ss.

«prevenire è meglio che curare». In definitiva, il principio di *accountability* consente di dare, con specifico riferimento al diritto di riservatezza e alla dignità della persona umana[63], concretezza a quelle proposte *de jure condendo* della moderna dottrina tese a garantire una tutela in chiave preventiva ai diritti della personalità. Con il nuovo regolamento, pertanto, si dispone della necessità di un controllo ispirato al principio di precauzione e di prevenzione con la previsione di doveri specifici imposti al titolare del trattamento, che attuano, per l'appunto, il principio di responsabilizzazione[64].

Interessante e calzante al fine di trarre delle conclusioni da quanto sinora affermato è la considerazione per la quale di là dalle soluzioni concrete e dai tecnicismi che gradualmente si svilupperanno, dal quadro complessivamente delineato, emerge un'importante evoluzione giuridica e culturale in atto, che parte dalla consapevolezza della centralità del tema della responsabilizzazione nel suo complesso e che vede consolidarsi il diritto fondamentale alla protezione dei dati personali attraverso una sua progressiva e crescente affermazione sul piano giuridico formale e sostanziale[65].

6. *Rilievi conclusivi.*

[63] P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, cit., p. 484, precisa opportunamente che il regolamento UE non è a tutela soltanto della riservatezza, ma esso disciplina piú ampiamente la dignità della persona umana.

[64] P. PERLINGIERI, *o.u.c.*, p. 481, il quale aggiunge che il regolamento contiene numerosi «princípi di valenza generale: il principio di proporzionalità – principio anche europeo, ormai fondamentale in tutti i settori della scienza giuridica dal tributario al penale, dall'amministrativo al civile –; il principio di trasparenza, che, pur trovando particolari recenti applicazioni nel diritto finanziario, riguarda l'intero sistema ordinamentale; il principio di effettività di rilevanza anche costituzionale; il principio di sussidiarietà, che – espressamente confermato dal regolamento UE – prevede l'intervento dell'Unione europea là dove difettino le normative nazionali del singolo Paese. Accanto a questi princípi comuni, caratterizzanti l'intero sistema ordinamentale, ne esistono specifici del settore, definibili speciali, come i princípi della finalità e della pertinenza, della minimizzazione e dell'anonimizzazione dei dati, intesa quale necessità di renderli per quanto piú possibile anonimi» (p. 482 s.). Sull'approccio di protezione preventivo che ammette l'affermazione di una «responsabilizzazione» del *provider* nell'educazione all'uso dei servizi offerti e sulla esperibilità del rimedio risarcitorio *ex* art. 2043 c.c. v. M. D'AMBROSIO, *Progresso tecnologico, «responsabilizzazione» dell'impresa ed educazione dell'utente*, cit., p. 79 ss.

[65] Quasi testualmente P. LA FARCIOLA, Data protection impact assessment *e sicurezza dei dati. Novità e criticità alla luce del principio di* accountability *nel Regolamento UE per la protezione dati personali 679/2016*, cit., p. 17.

Comune denominatore delle decisioni passate in rassegna è il principio di *accountability*: conferma, per così dire, applicativa del ruolo centrale assunto da tale principio nella riforma della disciplina in tema di protezione dei dati personali.

Le sanzioni irrogate per violazione dell'art. 32 GDPR stimolano un triplice ordine di considerazioni: il mancato adeguamento dei titolari del trattamento alla nuova disciplina nonostante la concessione del periodo di tolleranza, la conferma che la *compliance* al GDPR non può avvenire mediante un'attività, per così dire, *one shot* e la sensibilità mostrata dalla nostra Autorità di controllo e da quelle europee verso la necessità e l'urgenza, attesa la delicatezza delle questioni coinvolte, di responsabilizzare i titolari del trattamento.

Interessanti sono le parole dell'attuale Presidente del Garante *privacy* italiano Antonello Soro, il quale sottolinea come il regolamento europeo abbia «valorizzato in maniera determinante la "funzione sociale" della protezione dei dati personali, attribuendo un ruolo chiave e una più marcata responsabilità ad aziende e pubbliche amministrazioni» e configurato «la sanzione amministrativa come una delle possibili reazioni (non certo l'unica) all'illecito, da applicarsi con un approccio gradualistico, insieme o alternativamente alle misure inibitorie e prescrittive»[66]. È quindi pacifico che il momento nodale dell'irrogazione delle sanzioni amministrative corrisponde non tanto alla aprioristica e statica previsione normativa, bensì alla fase dinamica di valutazione e bilanciamento delle circostanze pertinenti della situazione specifica[67].

Da tali riflessioni emergono alcune considerazioni.

In primis, il GDPR ha aperto un nuovo scenario nel modello sanzionatorio in materia di protezione dei dati personali: dopo la sua entrata in vigore le Autorità di controllo europee hanno inflitto sanzioni che, è di tutta evidenza, non sarebbero state comminate o, comunque, avrebbero avuto dei tratti caratterizzanti diversi sotto la vigenza della disciplina anteriore. Quest'ultima, infatti, non discorreva di *accountability*, di *privacy by design* e *privacy by default*, di DPIA, di Registro dei trattamenti o di *data breach notification* e, dato da non sottovalutare, prevedeva misure di sicurezza, per così dire, più permissive. Ora, con questo non si vuol dire che le Autorità di controllo prima del

[66] Tratto dall'articolo *«Serve il salto di qualità sull'*accountability», pubblicato in *corrierecomunicazione.it*, 2019.

[67] V. BROVEDANI, *Le sanzioni amministrative nel GDPR*, in *cyberlaws.it*, 2019.

GDPR non avessero comminato sanzioni per la violazione delle misure di sicurezza, trascurando di vigilare sull'attenzione posta dai titolari sulle operazioni di elaborazione dei dati personali: si vuol soltanto sottolineare che le sanzioni inflitte per violazione delle misure di sicurezza – si pensi, ad esempio, alla violazione degli ormai abrogati artt. 31 (obblighi di sicurezza) o 33 (misure minime) del codice *privacy* (*ante* riforma) – si inserivano in un contesto diverso da quello attuale e assumevano un significato differente. Se le tecniche del *privacy by design* e *by default* erano già conosciute in precedenza (si pensi ai princípi di minimizzazione e di necessità disciplinati nel "vecchio" codice *privacy*), l'elemento di novità consiste nel fatto che con la nuova disciplina esse sono accolte nella sezione relativa agli obblighi generali posti in capo al titolare e al responsabile del trattamento: i nuovi strumenti in esame sono tutti fondati su un'attenta valutazione dei rischi di violazione dei diritti e delle libertà fondamentali delle persone interessate, sulle cui basi sorge l'obbligo per il titolare di predisporre misure e soluzioni tecniche specificamente mirate alla tutela dei dati personali (i c.dd. servizi e prodotti *privacy oriented*)[68].

In secondo luogo e facendo séguito alle parole del Presidente Soro, i Garanti europei hanno inflitto le sanzioni pecuniarie, le quali si pongono al vertice della piramide delle sanzioni irrogabili e puniscono le violazioni reputate più gravi, quando ad essere oltraggiato è stato il principio di *accountability*. Ciò a testimonianza della particolare sensibilità mostrata dalle Autorità di controllo verso la necessità di dare concreta attuazione all'obiettivo precipuo della nuova normativa: il radicale mutamento di prospettiva, il passaggio da un approccio fondato sulla riparazione del danno (*ex post*) a uno basato sulla prevenzione dello stesso (mediante una valutazione *ex ante* della rischiosità del trattamento). Se tale sensibilità merita di certo un plauso, qualche perplessità suscita invece la "clemenza" dimostrata dalle Autorità di controllo nel comminare le predette sanzioni: queste ultime, infatti, sono indiscutibilmente molto lontane dagli importi previsti dal GDPR. Tale circostanza trova una sua valida giustificazione: quasi tutte le sanzioni passate in rassegna sono state inflitte nel periodo di tolleranza. Con specifico riferimento al caso Rousseau rileva un'ulteriore circostanza segnalata dallo stesso Garante: «deve prendersi atto del percorso di progressivo

[68] In questi termini M.G. STANZIONE, *Il regolamento europeo sulla* privacy*: origini e ambito di applicazione*, cit., p. 1249 ss.

adeguamento e miglioramento delle misure di sicurezza adottate al fine di rafforzare la resilienza della piattaforma». Confermerebbe l'ipotesi qui avanzata la circostanza che la sanzione irrogata a TIM s.p.a., al termine del periodo di tolleranza, è nettamente più elevata, anche se, a dirla tutta, è lontana dai massimali contemplati dal GDPR che prevedono multe fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente.

A queste considerazioni, le quali consentono di dare una risposta affermativa al quesito con il quale si è dato il via all'indagine, si aggiungono le valutazioni di chi evidenzia le ulteriori significative innovazioni introdotte dal regolamento UE n. 679/2016: sotto il profilo metodologico, si rinviene una marcatura molto forte dei diritti dell'interessato all'accesso, al blocco, alla rettifica, alla cancellazione dei dati e anche del diritto a riceverli in formato strutturato affinché si possano trasmettere ad altri liberamente. L'informazione, pertanto, è considerata non soltanto in maniera statica quanto e soprattutto come insieme di dati in movimento e, come tali, idonei a tramutarsi, per connessione, in nuove e più sofisticate informazioni. L'innovazione configura il passaggio da una concezione fondata in via esclusiva sul consenso informato a una concezione caratterizzata prevalentemente sul controllo, nella consapevolezza che il consenso non è sufficiente e che anzi è, per certi versi, fuorviante e non idoneo di fatto a garantire il rispetto della persona. Il processo evolutivo, realizzato in questa materia, va di pari passo con l'affermarsi delle tradizioni costituzionali europee, con la prevalenza del riconoscimento e della garanzia dei diritti inviolabili della persona umana su altri istituti pur definiti fondamentali, ma non inviolabili: inviolabile in maniera assoluta è esclusivamente il valore della persona umana, il suo sviluppo, la sua dignità[69].

In definitiva si può concludere che il regolamento ha permesso di compiere dei passi in avanti in materia di protezione dei dati personali anche e soprattutto mediante l'opera delle Autorità di controllo le quali, sebbene non abbiano mostrato un "pugno di ferro" e siano risultati notevolmente indulgenti nella comminazione delle sanzioni, hanno mostrato una spiccata sensibilità verso il nucleo propulsore della nuova

[69] Come si è già avuto modo di chiarire (vedi *supra*, nota 60), il regolamento disciplina, oltre alla riservatezza, anche la dignità della persona umana. La ricostruzione delle ulteriori innovazioni introdotte dalla disciplina europea è di P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, cit., pp. 481 e 483 s.

disciplina europea: la responsabilizzazione di chi tratta i nostri dati personali, nella convinzione che la prevenzione sia la strategia più efficace per rinvigorire quella ormai sempre più flebile sfera privata.

In conclusione come si è molto ben rilevato in dottrina: «[i]l sistema europeo […] si mostra maggiormente coerente con la realtà tecnologica che intende disciplinare impostando criteri piú realistici, quali il controllo, piuttosto che il consenso, dal lato dell'interessato e un rafforzamento del binomio libertà/responsabilità, dal lato del titolare del trattamento»[70].

dirittifondamentali.it

[70] A.C. NAZZARO, *L'utilizzo dei* Big data *e i problemi di tutela della persona*, cit., p. 1259 s.