IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
ISSN
Anno XXXIV Fasc. 4-5 - 2019

Maria Samantha Esposito

TRATTAMENTO DEI DATI PERSONALI E RISCHI CORRELATI, NEL PRISMA DEI DIRITTI E DELLE LIBERTÀ FONDAMENTALI

Estratto

GIUFFRÈ FRANCIS LEFEBVRE

MARIA SAMANTHA ESPOSITO

TRATTAMENTO DEI DATI PERSONALI E RISCHI CORRELATI, NEL PRISMA DEI DIRITTI E DELLE LIBERTÀ FONDAMENTALI

1. Introduzione.

Il presente contributo si inserisce nel recente filone di studi in materia di trattamento dei dati personali che guarda ad un ampliamento della tutela riconosciuta dall'ordinamento, sia sul piano dei soggetti tutelati — dalla dimensione individuale a quella collettiva —, sia degli interessi tutelati, a favore di una più ampia gamma di diritti e libertà fondamentali.

In questa prospettiva, la prima parte del contributo sottolinea come l'approccio tradizionale in materia di protezione dei dati personali sia rivolto principalmente ai profili inerenti alla qualità e alla sicurezza dei dati, al fine di garantire la tutela del riserbo e delle informazioni dell'interessato. In questo contesto vengono poste in luce le nuove esigenze derivanti dall'attuale scenario

* Il presente lavoro è stato preventivamente sottoposto a referaggio anonimo affidato a un componente il Comitato Scientifico dei Referenti della Rivista secondo le prassi correnti nella comunità dei giuristi.

** Il presente contributo riprende e amplia gli spunti presentati nel corso della relazione tenuta in occasione del Convegno organizzato dall'Università di Pisa "*L'entrata in vigore del Regolamento (UE) 2016/679: la riforma alla prova della prassi in Italia e in Spagna. 1° Incontro di studi italo-spagnolo in materia di protezione dei dati personali*", Pisa, 8-9 giugno 2018. La ricerca è stata svolta nell'ambito del progetto H2020 Virt-EU (grant agreement No. 732027, responsabile scientifico per il Politecnico di Torino: Prof. Alessandro Mantelero).

tecnologico e informatico, le quali suggeriscono di considerare i nuovi potenziali pregiudizi derivanti dall'impiego delle informazioni personali.

Il terzo paragrafo si sofferma, quindi, sulle più recenti elaborazioni del concetto di rischio derivante dall'uso dei dati, emerse da più parti a livello europeo, mentre nel quarto e quinto paragrafo viene descritta la ricerca condotta attraverso l'esame delle decisioni e delle linee di indirizzo adottate nel corso del tempo da parte delle autorità preposte alla protezione dei dati personali in Italia e in Spagna. In questo contesto, viene in particolare evidenziata l'attenzione da parte delle autorità garanti esaminate verso una pluralità di diritti e libertà fondamentali, suscettibili di venire in considerazione nel caso concreto.

Da ultimo vengono formulate alcune considerazioni conclusive in merito alla necessità di adottare un approccio più ampio nella valutazione del rischio derivante dall'uso dei dati, e alla conseguente opportunità di elaborare un modello di analisi e gestione dei rischi che tenga conto, non solo dei tradizionali profili inerenti alla tutela della riservatezza e delle informazioni personali, ma altresì, di tutti i diritti e le libertà fondamentali dell'interessato suscettibili di subire un pregiudizio in occasione di un determinato trattamento.

2. L'approccio tradizionale in materia di analisi e gestione del rischio derivante dal trattamento dei dati personali e il nuovo contesto tecnologico e informatico.

Il rischio connesso all'impiego delle informazioni personali rappresenta un elemento centrale della disciplina sulla protezione dei dati fin dalle sue origini. L'approccio tradizionale in materia di analisi e gestione del rischio nel contesto della tutela dei dati personali è tuttavia caratterizzato dall'attenzione rivolta prevalentemente alla dimensione individuale e, in particolare, alla tutela della riservatezza e delle informazioni inerenti al singolo interessato.

Tale impostazione, se trovava la propria giustificazione nello scenario tecnologico esistente al momento dell'introduzione delle prime normative in materia di tutela dei dati personali [1], non

[1] Per un'analisi dei diversi scenari tecnologici e normativi susseguitesi nel tempo a partire dall'introduzione dei primi elaboratori elettronici, cfr., A. Mantelero, *La gestione del rischio* , in G. Finocchiaro (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* Bologna, 2018, 477 ss.; Id., *The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Comp. Law & Sec. Rev.*, 2014, 30, 647 e ss.

sembra adattarsi, invece, alle esigenze derivanti dall'attuale contesto tecnologico e informatico, ove la presenza di innovazioni sempre più complesse costringe a riflettere sulla necessità di valutare i nuovi potenziali pregiudizi che possono derivare dall'uso dei dati.

Attraverso l'impiego delle nuove tecnologie è invero possibile raccogliere e analizzare grandi masse di dati (c.d. *big data analytics*), trarne informazioni di carattere predittivo in merito alle scelte e ai comportamenti degli interessati, avvalersi di sistemi informatizzati di supporto alle decisioni o di processi decisionali automatizzati [2]. Tale crescente ricorso ai dati ed alla loro elaborazione mediante algoritmi a fini decisionali può tuttavia condurre a conseguenze negative per i diritti e le libertà dei soggetti coinvolti, incidendo sulla libertà di autodeterminazione e sul diritto al rispetto della dignità umana ai medesimi riconosciuti [3].

In questo contesto può considerarsi, tra l'altro, il rischio di

[2] Per alcuni esempi cfr., tra gli altri, D. K. Citron, F. Pasquale, *The scored society: due process for automated predictions*, *Wash. Law Rev.*, 2014, 89, I, 2 ss.; T. Z. Zarsky, *Transparent Predictions*, in *University of Illinois L. Rev.*, 2013, 4, 1510 e ss..

[3] Con riferimento ai pregiudizi che possono derivare da queste nuove forme di trattamento, cfr., *ex multis*, V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, London, 2013, 150 e ss.; K. Krasnow Waterman, P. J. Bruening, *Big Data analytics: risks and responsibilities*, in *Int. Data Privacy Law*, 2014, 4, 2, 89 e ss.; F. Bosco et al., *Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities*, in S. Gutwirth et al. (eds), *Reforming European Data Protection Law*, Springer, Dordrecht, 2015, 11 ss.; D. Bollier, *The Promise and Peril of Big Data*, Washington, DC, 2010, consultabile all'indirizzo: *http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf*; S. Niger, *Sorveglianza e nuovi diritti di libertà*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in *Tratt. dir. comm. e dir. pubb. econ.*, diretto da F. Galgano, Padova, 2008, 12 e ss., il quale evidenzia, in particolare, i rischi di « schedatura sociale », che possono derivare dalle attività di profilazione degli utenti, le quali non considerano i diritti degli individui e riducono le informazioni che li riguardano a « merce »; V. Zeno Zencovich, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Riv. dir. media*, 2018, 2, 5 e ss.; Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, Strasburgo, 23 gennaio 2017, consultabili al seguente indirizzo: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a*; A. Rouvroy, *"Of data and men". Fundamental rights and freedoms in a world of big data*, Council of Europe, Directorate General of Human Rights and Rule of Law, Strasburgo, 11 gennaio 2016, consultabile all'indirizzo: *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020*; Council of Europe, Committee of Experts on Internet Intermediaries, *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*, Strasburgo, 2017, consultabile all'indirizzo: *https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5*. In argomento, cfr., altresì, S. Perry, C. Roda, *Human Rights and digital*

controllo individuale e sociale [4] che può derivare dai dispositivi IoT (*Internet of Things*), sempre più estensivamente impiegati per la raccolta dati. È il caso ad esempio, dei c.d. contatori intelligenti, in grado di raccogliere informazioni dettagliate sul consumo energetico tali da rivelare le abitudini, le condizioni di salute ovvero altre caratteristiche relative ai comportamenti degli utenti [5].

technology, London, 2017, 63 e ss., ove si evidenzia come l'analisi dei *big data* non consente solamente di ottenere vantaggi di tipo economico ma anche di tipo politico, stante la possibilità di influenzare e, in alcuni casi, di controllare, i comportamenti degli utenti; F. A. Raso, H. Hilligoss, V. Krishnamurthy, C. Bavitz, L. Kim, *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet & Society at Harvard University, *Research Publication n. 6-2018*, September 25, 2018, consultabile all'indirizzo: *https://cyber.harvard.edu/publication/2018/artificial-intelligence-human-rights*; Federal Trade Commission, *Big Data: A tool for Inclusion or Exclusion? Understanding The Issues*, Report, Gennaio 2016, consultabile al seguente indirizzo: *https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf*; European Data Protection Supervisor, *Towards a new digital ethics. Data, dignity and technology*, Opinion 4/2015, consultabile all'indirizzo: *https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf*: « Profiles used to predict people's behaviour risk stigmatisation, reinforcing existing stereotypes, social and cultural segregation and exclusion, with such 'collective intelligence' subverting individual choice and equal opportunities »; European Union Agency for Fundamental Rights, *Handbook on European data protection law*, 2018, 347 ss., spec. 354, consultabile all'indirizzo: *http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition*; International conference of Data Protection & Privacy Commissioners, *Resolution on Big Data*, 2014, in *https://icdppc.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf*. Tutti i siti web richiamati nel presente lavoro sono stati consultati fra il 5 marzo e il 15 novembre 2018.

[4] In generale, con riferimento ai rischi di sorveglianza e di controllo sociale derivanti dall'evoluzione delle tecnologie, cfr., S. Niger, *Sorveglianza e nuovi diritti di libertà*, cit., 7 ss.; F. H. Cate, *Government Data Mining: The Need for a Legal Framework*, Articles by Maurer Faculty. Paper 150, 2008, 477 e ss., consultabile all'indirizzo: *https://www.repository.law.indiana.edu/facpub/150/*, ove si evidenzia, in particolare, come il timore di essere sorvegliati da parte dei pubblici poteri induca inevitabilmente la popolazione a cambiare i propri comportamenti e a ridurre le proprie attività all'interno della società. Con riferimento al rischio di monitoraggio suscettibile di venire in considerazione in occasione di determinati trattamenti, cfr., altresì, A. Mantelero, *Data protection, e-ticketing, and intelligent systems for public transport*, in *Int. Data Privacy Law*, 2015, V, 4, 309 e ss. In particolare, l'A. prende in considerazione i sistemi di mobilità intelligente, i quali, attraverso la raccolta di una pluralità di dati riguardanti, tra l'altro, il traffico, le abitudini e i percorsi maggiormente richiesti dagli utenti, sono in grado di offrire agli utenti servizi più efficienti. Tali sistemi, tuttavia, stante la loro capacità di localizzare, tracciare e registrare le abitudini dei passeggeri, sono suscettibili di sottoporre questi ultimi a forme di sorveglianza invasive. In generale, con riferimento al controllo sociale da parte dei pubblici poteri, reso possibile dalla raccolta di una pluralità di dati concernenti i cittadini, da parte, tra l'altro, delle compagnie private, cfr., A. Mantelero, G. Vaciago, *The* "Dark Side" *of Big Data*: *Private and Public Interaction in Social Surveillance. How data collections by private entities affect governmental social control and how the EU reform on data protection responds*, in *Comp. Law Rev. Int.*, 6, 2013, 161 e ss.

[5] In proposito, cfr., V. Mayer- Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, cit., 152 s.; Article 29 Data Protection Working Party, *Opinion 12/2011 on smart* metering, WP 183, del 4 aprile 2011; Article 29-Data Protection Working Party, *Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force*, WP 205, del 22 aprile 2013. I documenti adottati dall'Article 29-Data Pro-

Sempre più frequentemente, inoltre, oggetto di attenzione non è più il singolo quanto, piuttosto, la società nel suo insieme o determinati gruppi di individui, dei quali vengono individuate caratteristiche comuni, preferenze e abitudini, al fine di predirne i futuri comportamenti ovvero adottare decisioni che interessano tutta la comunità considerata [6].

Al riguardo, occorre altresì porre in luce come le conseguenze dell'utilizzo di soluzioni di *big data analitycs*, nella maggior parte dei casi, non riguardino gruppi preesistenti di individui, quanto, piuttosto, collettività derivanti dall'aggregazione dei dati raccolti, realizzata mediante l'impiego di determinati algoritmi. I gruppi oggetto di analisi, infatti, sono spesso creati dagli stessi titolari del trattamento sulla base delle particolari informazioni prese in considerazione; di conseguenza, in tali ipotesi, sono le stesse caratteristiche dei gruppi, e non dei singoli individui che li compongono, ad essere poste a fondamento delle decisioni ovvero delle previsioni formulate sulla base di correlazioni [7].

Per tale via, le decisioni e le previsioni assunte dai titolari in virtù delle inferenze emerse dall'analisi dei gruppi possono dar luogo a forme di pregiudizio che non colpiscono, ovvero che non

---

tection Working Party, richiamati nel presente lavoro, sono consultabili all'indirizzo *https://ec.europa.eu/justice/article-29/documentation/index_en.htm*, con riferimento ai documenti adottati fino al mese di ottobre 2016, e all'indirizzo *https://ec.europa.eu/newsroom/article29/news-overview.cfm*, per i documenti adottati successivamente a tale data. In generale, con riferimento alla molteplicità di implicazioni derivanti a danno della sfera privata dai dispositivi dotati di intelligenza artificiale impiegati all'interno delle case, cfr., S. De Conca, *From the glass house to the hive: the private sphere in the era of intelligent home assistant robots*, in M. Hansen, E. Kosta, I. Nai-Fovino, S. Fischer-Hübner (eds.), *Privacy and Identity Management: the Smart Revolution*, Springer International Publishing, 2018, 282 e ss.

[6] In proposito possono richiamarsi i sistemi per l'analisi dei *big data* impiegati per predire il verificarsi di crimini in determinate aree (sull'argomento, cfr., tra gli altri, W. L. Perry, B. McInnis, C. C. Price, S. C. Smith, J. S. Hollywood, *Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, CA, 2013, consultabile all'indirizzo: *https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf*; D. Robinson, H. Yu, A. Rieke, *Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology*, 2014, 18-19, consultabile all'indirizzo: *https://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf*), ovvero per suddividere la clientela secondo precise categorie da parte delle imprese di assicurazione o enti creditizi (in argomento cfr., *ex multis*, Federal Trade Commission, *Credit-Based Insurance Scores: Impacts on consumers of automobile insurance*, Report to Congress - July 2007, 50 ss., in *https://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf*).

[7] Per un'ampia indagine in merito alla differenza tra il gruppo tradizionalmente inteso, quale somma dei membri che lo compongo, e il gruppo generato dall'impiego degli algoritmi, cfr., A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Comp. Law and Sec. Rev.*, 2016, 32, 241 e ss.; Id., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in L. Taylor, L. Floridi, B. van der Sloot (eds), *Group Privacy. New Challenges of Data Technologies*, Springer International Publishing, 2017, 139 e ss.

colpiscono solamente, il singolo membro, quanto, piuttosto, il gruppo in sé considerato.

In questo contesto, le conseguenze negative che possono interessare tali gruppi riguardano principalmente i pregiudizi derivanti da forme di trattamento di natura discriminatoria o invasiva [8] e non, dunque, i danni derivanti dal trattamento illegittimo di dati o dall'assenza di segretezza, oggetto, invece, di tradizionale tutela.

Questo comporta l'emergere di un interesse rispetto ad un corretto uso delle informazioni raccolte che va al di là dell'individuo e, di conseguenza, l'esigenza di riconoscere, accanto alla dimensione individuale della tutela dei dati, che ha riguardo ai diritti del singolo e alle informazioni che lo riguardano, altresì, la dimensione collettiva.

Le sfide poste dal trattamento dei dati, inoltre, non interessano solo forme intensive di trattamento, quali quelle derivanti dall'analisi dei *big data* e dall'impiego di sistemi di intelligenza artificiale, ma anche nuove opportunità ed applicazioni di tecnologie più tradizionali, spesso anche meno costose rispetto alle prime e, di conseguenza, potenzialmente maggiormente diffuse. In questo senso vengono in considerazione, ad esempio, gli strumenti utilizzati per la raccolta di dati di carattere biometrico, i sistemi di videosorveglianza intelligente, i sistemi RFID [9] ovvero i sistemi GPS o, ancora, i *wereable devices* [10].

---

[8] In proposito cfr., A. Mantelero, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, in *Contr. Impr. Eur.*, 2015, 1, 142 e ss., ove a titolo semplificativo si richiama il *software* "PredPol" in uso da parte delle forze di polizia locale statunitense, in grado di anticipare e prevenire futuri crimini mediante un controllo incrociato di dati, luoghi e tecniche relativi a crimini già commessi. Al riguardo, l'A. evidenzia, in particolare, come tali sistemi rischino di autogenerare determinate previsioni, dal momento che, ad esempio, i servizi di polizia saranno indotti a collocare maggiori risorse nelle aree suggerite dall'analisi, con la conseguenza di favorire l'accertamento dei reati in quelle zone e di rafforzare, dunque, la previsione originaria; S. Barocas, A. D. Selbst, *Big Data's Disparate Impact*, in *California Law Rev.*, 2016, 104, 671 ss. Con riferimento al rischio di discriminazione derivante da queste nuove forme di classificazione delle persone cfr., altresì, G. Comandè, *Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems, and Opportunities of Algorithms*, in T. Cerquitelli, D. Quercia, F. Pasquale (eds), *Transparent Data Mining for Big and Small Data*, Springer International Publishing, 2017, 172 ss.; B. Lepri et al., *The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good*, *ivi*, 13 e ss.; The White House, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, 2014, 51 e ss., consultabile all'indirizzo: *https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf*; Id., *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, 2016, consultabile al seguente indirizzo: *https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf*.

[9] Il *Radio Frequency Identification* (RFID) è una tecnologia che usa onde elettromagnetiche per l'identificazione automatica di cose o persone. Il sistema — che può essere collegato o meno con le infrastrutture di rete (telefonia, Internet, ecc.) — si compone di un Tag (ossia un'etichetta costituita da una memoria elettronica leggibile e, in alcuni casi, altresì, scrivibile, nonché da antenne), il quale può contenere un codice identificativo ovvero ulteriori informazioni, e di un lettore (c.d. *reader*). I lettori RFID consentono, dunque, di leggere le informazioni contenute nei Tag. Tale tecnologia viene

In proposito, possono annoverarsi i sistemi di localizzazione dei veicoli aziendali, i quali vengono impiegati nell'ambito del rapporto di lavoro al fine di rendere maggiormente efficienti determinate attività e/o di garantire la sicurezza dei lavoratori ovvero degli stessi veicoli contro eventuali furti [11]. Tali sistemi, stante la loro capacità di dar luogo a forme di controllo a distanza, possono invero risolversi — anche in considerazione delle modalità con le quali vengono in concreto impiegati — in forme di condizionamento, tali da incidere, tra l'altro, sulla libertà di autodeterminazione e di movimento dei lavoratori.

Ancora, possono richiamarsi i braccialetti elettronici ed i *microchips* sottocutanei — il cui uso è emerso sempre nel contesto lavorativo al fine di facilitare, monitorare e guidare l'attività dei dipendenti —, dal momento che possono parimenti condurre a gravi forme di condizionamento, limitando l'autonomia degli interessati e finanche la loro dignità [12].

L'esame dell'attuale contesto tecnologico e informatico mette in luce, dunque i limiti che caratterizzano l'approccio tradizionale in materia di tutela dei dati personali, con particolare riferimento all'analisi e gestione del rischio. Emerge, di conseguenza, l'esigenza di elaborare modelli operativi che tengano conto dei nuovi potenziali effetti negativi derivanti dall'uso dei dati e guardino

sempre più spesso impiegata, ad esempio, per assicurare una migliore gestione della produzione, delle operazioni di consegna delle merci ovvero per controllare gli accessi in luoghi riservati. Con riferimento ai rischi che possono derivare per i diritti e le libertà fondamentali degli interessati dall'impiego dei sistemi RFID, cfr., *ex multis*, Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, WP105, del 19 gennaio 2005.

[10] Con riferimento ai rischi derivanti dall'impiego dei dati raccolti dai dispositivi indossabili, cfr., tra gli altri, K. Montgomery, J. Chester, K. Kopp, *Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment*, in *Journal Inf. Pol.*, 8, 2018, 34 ss.

[11] Al riguardo, cfr., *ex multis*, Garante per la protezione dei dati personali, 7 ottobre 2010, doc. web n. 1763071; Garante per la protezione dei dati personali, 4 ottobre 2011, n. 370, doc. web n. 1850581. Tutti i provvedimenti e i documenti di indirizzo adottati dall'Autorità garante italiana e richiamati nel presente lavoro sono consultabili sul sito Internet della medesima autorità: *https://www.garanteprivacy.it*.

[12] Al riguardo, cfr. le osservazioni del Garante italiano in: P. Baroni "*Da noi è vietato robotizzare l'uomo*" — intervista ad A. Soro, Presidente del Garante per la protezione dei dati personali, in *La Stampa*, 3 febbraio 2018, consultabile su *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7712329*. In generale, con riferimento al crescente controllo dei lavoratori conseguente al sempre maggior impiego di strumenti informatici nell'ambiente produttivo, cfr., tra gli altri, G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, in P. Tullini (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, Torino, 2017, 51 e ss.; D. Poletti, *Il c.d. diritto alla disconnessione nel contesto dei « diritti digitali »*, in *Resp. civ. e prev.*, 2017, 1, 8 e ss.; S. Niger, *Controllo dei lavoratori, videosorveglianza, anonimato*, in G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, cit., 223 e ss.; P. Tullini, *La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa*, in P. Tullini (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, cit., 3 e ss.; M. Aimo, *Tutela della riservatezza e protezione dei dati personali dei lavoratori*, in M. Marazza (a cura di), *Contratto di lavoro e organizzazione*, II, in M. Persiani, F. Carinci, *Tratt. dir. lav.*, IV, Padova, 2012, 1307 e ss.

oltre la sola sfera dell'autodeterminazione informativa o della riservatezza, per ricomprendere altri diritti e libertà fondamentali dell'interessato, messi a rischio dalle nuove invasive e pervasive forme di trattamento, sia su base individuale che collettiva.

3. La recente elaborazione del rischio connesso all'uso delle informazioni personali nel contesto europeo.

L'esigenza di una più ampia interpretazione della nozione di rischio è emersa già da tempo in alcuni contributi dottrinali [13], nonché in diversi progetti di ricerca a livello europeo incentrati sulla valutazione etica della ricerca e dell'innovazione [14].

In particolare, con riferimento al tema specifico della tutela dei dati personali, numerosi interventi, nel porre in luce le diverse questioni sollevate dall'impiego delle nuove tecnologie, hanno esortato l'adozione di differenti modelli di valutazione di impatto in grado di considerare, altresì, la pluralità di diritti umani e

[13] Cfr., tra gli altri, A. H. Vedder, *Privatization, Information Technology and Privacy: Reconsidering the Social Responsibilities of Private Organizations*, in G. Moore (ed), *Business Ethics: Principles and Practice*, Sunderland, Business Education Publishers, 1997, 215 ss.; D. Wright, *A framework for the ethical impact assessment of information technology*, in *Ethics inf. Technol.*, 2011, 13, 199 ss.; C. Raab, D. Wright, *Surveillance: Extending the Limits of Privacy Impact Assessment*, in D. Wright, P. De Hert (eds), *Privacy Impact Assessment*, Springer, Netherlands, 2012, 363 e ss.; D. Wright, E. Mordini, *Privacy and Ethical Impact Assessment*, *ivi*, 397 e ss.; D. Wright, M. Friedewald, *Integrating privacy and ethical impact assessments*, in *Science Publ. Pol.*, 2013, 40, 755 e ss., consultabile all'indirizzo: *https://www.dhi.ac.uk/san/waysofbeing/data/data-crone-wright-2013.pdf*, ove si evidenzia in particolare che: « *it becomes clear that many of the privacy problems produced by new technologies can no longer be adequately assessed and addressed with revised data protection approaches alone. With the advent of new technologies such as next-generation biometrics, DNA sequencing and human enhancement technologies, the data being collected moves from simply describing a person to being an inherent part of the person* (...). *All these challenges make it necessary not only to broaden data protection procedures and regulations but also to take other human values and rights into account to support policymakers and decision-takers to better balance countervailing interests* »; L. Taylor, L. Floridi, B. van der Sloot (eds), *Group Privacy. New Challenges of Data Technologies*, Springer, 2017; A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, cit., 238 e ss.; nonché, più recentemente, Id., *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, in *Comp. Law & Sec. Rev.*, 34, 2018, 754 e ss., ove l'A. propone un modello di valutazione di impatto (c.d. HRESIA-*Human Rights, Ethical and Social Impact Assessment*) che, oltre a considerare i tradizionali rischi legati alla qualità e alla sicurezza dei dati, tenga conto, altresì, dei diritti fondamentali suscettibili di subire un pregiudizio nel contesto di un determinato trattamento. In particolare, nel modello proposto tali diritti umani vengono presi in considerazione e valutati, altresì, alla luce dei valori etici e sociali diffusi all'interno del particolare contesto di riferimento; B. Carsten Stahl, D. Wright, *Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation in AI-related projects*, in *ISEE Sec. Priv.*, 16, 3, 2018.

[14] Cfr., tra gli altri, Progetto europeo H2020 SATORI "*Stakeholders Acting Together on the Ethical Impact Assessment of Research and Innovation*", consultabile al seguente all'indirizzo: *http://satoriproject.eu/*; Progetto europeo H2020 Virt-EU "*Values and ethics in Innovation for Responsible Technology in Europe*", consultabile all'indirizzo: *https://virteuproject.eu/*.

valori etico-sociali suscettibili di subire un pregiudizio in occasione di un determinato trattamento dei dati personali.

In questo contesto, l'opportunità di una valutazione più ampia dei rischi correlati all'uso delle informazioni sembra aver trovato un primo concreto riconoscimento normativo all'interno del Regolamento (UE) 2016/679 [15]. Nello specifico, come confermato dall'Article 29 Data Protection Working Party [16], il riferimento ai diritti e alle libertà delle persone, contenuto nel considerando n. 75 e nell'art. 35, nonché in altre disposizioni della nuova disciplina [17], sembra suggerire una lettura della nozione di rischio non più circoscritta ai soli profili inerenti alla protezione dei dati e alla riservatezza dell'interessato, ma estesa, altresì, ad ulteriori diritti e libertà fondamentali, quali la libertà di movimento, di pensiero, di coscienza e di religione o, ancora, la libertà da discriminazione [18].

E tuttavia, nonostante il Regolamento (UE) 2016/679 sembri muoversi nella direzione favorevole ad una più ampia considerazione dei rischi concernenti l'uso dei dati, le previsioni in materia di valutazione e gestione del rischio ivi contenute risultano ancora

[15] In proposito, può altresì osservarsi come il profilo del rischio e della sua gestione — senz'altro già elemento essenziale nell'ambito delle diverse normative in materia di protezione dei dati personali — rappresenti un elemento centrale all'interno del Regolamento, maggiormente incentrato sul principio di *accountability* e di prevenzione del danno. In questa prospettiva possono richiamarsi le nuove disposizioni relative all'analisi dei rischi, ovvero quelle sulla valutazione d'impatto e sulla consultazione preventiva delle autorità garanti (cfr. in particolare i considerando nn. 75 e 76 e gli artt. 35 e 36). Per tali considerazioni, cfr., tra gli altri, G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, I, 10; Id., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* , cit., 17 s.; Recio Gayo M., *Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control*, in *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, diretto da J. L. Piñar Mañas e coordinato da M. Álvarez Caro, M. Recio Gayo, Madrid, 2016, 355.

[16] Cfr., Article 29 Data Protection Working Party, "*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679*", adottate il 4 aprile 2017 e da ultimo modificate e adottate il 4 ottobre 2017 (al riguardo, cfr. le osservazioni di R. Gellert, *The Article 29 Working Party's Provisional Guidelines on Data Protection Impact Assessment*, in *European Data Protection Law Rev.*, 2017, III, 2, 212 ss.).

[17] Cfr., in particolare, artt. 24 e 32, Regolamento (UE) 2016/679. In questo contesto, inoltre, l'espresso rinvio a « qualsiasi altro danno economico o sociale », formulato all'interno del considerando n. 75, assume particolare importanza nell'attuale contesto tecnologico e informatico contraddistinto dal sempre maggior impiego dei *big data* e dei processi decisionali che sugli stessi si basano, suscettibili di dar luogo a pregiudizi di carattere discriminatorio.

[18] Per tali osservazioni cfr., altresì, A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, I, 155; C. Quelle, *The "risk revolution" in EU data protection law: We can't have our cake and eat it, too*", in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds), *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, 2017, IV, consultabile all'indirizzo *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382*.

principalmente circoscritte alla tutela della sicurezza e della qualità dei dati. In particolare, nel contesto della disciplina introdotta dal legislatore europeo paiono essere carenti strumenti concreti in grado di far fronte alle nuove forme di pregiudizio che possono derivare dall'uso dei dati [19].

Una maggiore e più operativa presa di coscienza di queste istanze è emersa, invece, sia nelle più risalenti indicazioni in materia dell'Article 29 Data Protection Working Party [20] sia, in particolare, a livello di Consiglio d'Europa, laddove un ruolo di sicuro rilievo per una valutazione più ampia del concetto di rischio dev'essere senz'altro riconosciuto alle linee guida sui *big data* recentemente adottate [21].

Invero, proprio tali linee guida — dopo aver posto in luce i nuovi e diversi profili di criticità sollevati dalle forme di trattamento basate sull'analisi di grandi quantità di dati — sollecitano una valutazione dei rischi che tenga altresì conto della dimensione collettiva dell'uso delle informazioni, nonché delle conseguenze che possono derivare sotto il profilo etico e sociale [22].

Particolare rilevanza riveste, inoltre, l'accento posto sulla natura contestuale dei valori etici e sociali, rispetto alla quale le linee guida suggeriscono una valutazione di rischio incentrata non solo sui principi espressi dalle carte internazionali dei diritti e

---

[19] Sottolineano i limiti del modello adottato dal legislatore europeo, tra gli altri, A. Mantelero, *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, cit., 755 s.; Id., *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Comp. Law & Sec. Rev.*, 2017, 33, 588 ss.; V. Mayer-Schönberger, Y. Padova, *Regime Change? Enabling Big Data trough Europe's New Data Protection Regulation*, cit., 331 e ss.

[20] Cfr., Article 29 Data protection Working Party, "*Statement on the role of a risk-based approach in data protection legal frameworks*", adottato il 30 maggio 2014, 4, ove si evidenzia che: « *the scope of 'the rights and freedoms' of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion* », nonché che: « *The risk-based approach goes beyond a narrow "harm-based-approach" that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust)* ».

[21] Cfr., Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, cit., sez. IV, § 2.3. In proposito, cfr., più ampiamente, A. Mantelero, *Regulating big Data. The guidelines of the Council of Europe in the context of the European data protection framework*, cit., 584 ss.

[22] V., in particolare, Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, cit., sez. IV, § 2.3: « *Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the legal, social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to non-discrimination* ».

delle libertà fondamentali, ma anche sui valori diffusi all'interno delle singole comunità [23].

Un contributo importante nella direzione sopra delineata si rinviene, altresì, nella posizione assunta al riguardo dall'European Data Protection Supervisor. Quest'ultimo, in particolare, preso atto delle diverse questioni etiche che possono venire in considerazione nel contesto, ad esempio, dei *big data*, del *cloud computing*, dell'*Internet of things*, ovvero in occasione dell'impiego della biostampa 3D o delle tecniche di intelligenza artificiale, ha esortato un generale ripensamento del rapporto tra la tecnologia e i valori umani, al fine di assicurare il più ampio rispetto della dignità individuale [24].

4. Il ruolo dei diritti fondamentali nella giurisprudenza delle autorità garanti italiana e spagnola. Il metodo di indagine.

I recenti interventi menzionati nel precedente paragrafo consentono di confermare una generale acquisita consapevolezza dell'esistenza di nuovi e più ampi pregiudizi che possono derivare dall'uso dei dati nell'attuale contesto tecnologico e informatico.

I modelli di valutazione e gestione del rischio da ultimo proposti risultano, tuttavia, come detto, tutt'ora principalmente incentrati sull'esigenza di garantire la qualità e la sicurezza dei dati, in un'ottica di tutela del riserbo e delle informazioni inerenti all'interessato, tralasciando, invece, gli aspetti relativi alla natura degli ulteriori diritti umani e libertà fondamentali e alle eventuali implicazioni di tipo etico e sociale che possono venire in considerazione nel caso concreto, nonché i profili riguardanti la loro specifica tutela [25].

Queste considerazioni hanno portato ad indagare se e come una

[23] Cfr., Consultative Committee of the Convention for the Protection of Individuals with Regard to automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, cit., Sez. IV, § 1.2: « *Personal data processing should not be in conflict with the ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests, values and norms* ».

[24] Cfr., European Data Protection Supervisor, *Towards a new digital ethics. Data, dignity and technology*, cit. La riflessione avviata in materia da tale organo ha inoltre condotto l'EDPS alla costituzione di un Comitato consultivo *ad hoc*, con il compito di riconsiderare la dimensione etica dell'uso dei dati. In proposito, cfr., quanto osservato dal Comitato nel suo primo Report: EDPS Ethics Advisory Group, Report 2018, 6 ss., consultabile all'indirizzo *https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf*.

[25] Cfr., tra gli altri i modelli di valutazione di impatto elaborati dalle autorità garanti nazionali francese e spagnola: CNIL, *Privacy Impact Assessment (PIA). Knowledge Bases*, 2018, consultabile all'indirizzo: *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf*; CNIL, *Privacy Impact Assessment (PIA). Methodology*, 2018, in *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf*; CNIL, *Privacy Impact Assessment (PIA). Templates*, 2018, in *https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf*; Agencia Española de Pro-

valutazione maggiormente estesa delle implicazioni del trattamento dei dati, che includa tanto i diritti e le libertà dei singoli quanto le istanze etiche e sociali, abbia già trovato riscontro nella giurisprudenza delle autorità garanti nazionali [26], fornendo così elementi utili all'elaborazione di un più ampio modello di valutazione del rischio [27].

Nello specifico, l'obiettivo — perseguito mediante l'esame delle pronunce e delle linee di indirizzo adottate nel corso del tempo da parte delle autorità garanti nazionali — è stato quello di individuare la pluralità di diritti umani e libertà fondamentali suscettibili di venire in considerazione nel contesto dei diversi trattamenti dei dati personali. Tale indagine costituisce, infatti, la fase prodromica per poter poi elaborare un paradigma valoriale più esteso, suscettibile di essere impiegato nell'articolazione di un modello di *risk assessment* che sia in grado di dare una più compiuta risposta alla molteplicità delle implicazioni proprie delle attuali sofisticate e pervasive forme di uso dei dati [28].

Considerato il condizionamento che anche le libertà e i diritti fondamentali ricevono nel contesto sociale [29], e che tale condizionamento è ancor più evidente per i valori di tipo etico e sociale,

---

tección de Datos, *Guía Práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*, 2018, consultabile all'indirizzo: *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf*; Agencia Española de Protección de Datos, *Guía práctica para las evaluaciones de impacto en la protec- ción de los datos sujetas al RGPD*, 2018, in *https://www.agpd.es/ portalwebAGPD/canaldocumentacion/publicaciones/common/ Guias/2018/Guia_EvaluacionesImpacto.pdf*; Autoridad Catalana de Protección de Datos, *Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)*, 2018, in *http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_protecci_de_dades/documents/GUIA- EVALUACION-DE- IMPACTO- CAST- 2.0.pdf*.

[26] Tale attività rappresenta parte della ricerca svolta nell'ambito del Progetto europeo H2020 Virt-EU, cit., sui valori e l'etica nel contesto delle innovazioni tecnologiche e, in particolare, delle tecnologie IoT.

[27] In questo contesto può richiamarsi il modello HRESIA (*Human Rights, Ethical and Social Impact Assessment*) proposto da A. Mantelero, quale modello di analisi e gestione del rischio derivante dall'uso dei dati che tenga conto di tutti i diritti umani e le libertà fondamentali suscettibili di subire un pregiudizio in occasione di un determinato trattamento, considerati anche alla luce dei particolari valori etici e sociali diffusi all'interno del contesto di riferimento (in proposito, v., altresì, *supra*, *sub* nota 13). Per ulteriori esempi di modelli di valutazione del rischio in grado di considerare gli ulteriori — rispetto a quelli tradizionalmente tutelati — pregiudizi che possono derivare dall'impiego delle informazioni, cfr., tra gli altri, D. Wright, *A framework for the ethical impact assessment of information technology*, cit., 199 e ss., il quale, tuttavia — a differenza di quanto suggerito nel presente contributo —, prende in considerazione le sole implicazioni etiche che possono derivare dall'uso dei dati (c.d. *Ethical impact assessment*).

[28] In proposito, cfr., tra gli altri, quanto messo in luce nel contesto dei contributi richiamati *sub* note 3, 4 e 8.

[29] È evidente, infatti, come la diversa incidenza dei diritti e delle libertà fondamentali riconosciuti a ciascun individuo, inclusi il diritto alla riservatezza e alla tutela dei dati personali, sia determinata dal modo in cui gli stessi sono avvertiti all'interno del contesto sociale e in relazione a quel dato momento storico. In merito all'esigenza di considerare il contesto sociale di riferimento, cfr., tra gli altri, H. Nissenbaum, *Privacy in Context. Technology, Policy and the Integrity of Social Life*, Stanford, 2010; A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an*

nel condurre questa prima indagine in materia si è preferito ridurre tale eventuale complessità derivante dal dato contestuale, circoscrivendo l'analisi alla giurisprudenza delle autorità preposte alla protezione dei dati personali in Italia e in Spagna. Questo in ragione sia della comunanza che connota gli ordinamenti di tali Paesi, tanto sul piano giuridico quanto su quello dei più ampi valori socioculturali, sia dell'affinità del *modus operandi* di tali autorità (con riferimento, ad esempio, sia all'ampia casistica giurisprudenziale sia alla presenza di linee guida e di documenti di indirizzo).

In questo contesto, una prima selezione delle decisioni assunte nel corso del tempo da tali autorità è stata fatta mediante il ricorso alle parole chiave ritenute maggiormente pertinenti rispetto alla tematica oggetto della ricerca. L'attenzione è stata rivolta, in particolare, alla diversa natura degli strumenti impiegati ai fini della raccolta dei dati — considerandone l'invasività e l'ampiezza (ad esempio: sistemi di videosorveglianza; sistemi di geolocalizzazione; strumenti per la raccolta di dati biometrici) —, alla natura dei luoghi (ad esempio: luoghi pubblici o privati) e al contesto di riferimento (ad esempio, il rapporto di lavoro). Si è guardato, inoltre, alla natura dei soggetti coinvolti (quali i soggetti deboli) e alla posizione dai medesimi assunta rispetto ai titolari del trattamento (con riferimento, ad esempio, alle ipotesi in cui sussistano squilibri di potere).

All'esito di questa indagine iniziale — elaborata sulla base dei documenti messi a disposizione da parte delle autorità garanti sul proprio sito Internet sono stati selezionati circa 300 provvedimenti, di cui circa 220 adottati dal Garante italiano e i restanti emessi, invece, dall'autorità garante spagnola.

Tali provvedimenti — previa eliminazione dei documenti ridon-

individual to a collective dimension of data protection, cit., 249, il quale, a titolo esemplificativo, evidenzia come « *There are jurisdictions that give greater priority to national and security interests, which in many cases prevail over individual and collective data protection; meanwhile, in some countries extensive forms of social surveillance are considered disproportionate and invasive* »; Id., *Data protection, e-ticketing, and intelligent systems for public transport*, cit., 310. Al riguardo, cfr., altresì, D. Wright, *A framework for the ethical impact assessment of information technology*, cit., 200. In generale, in merito alla variabilità con la quale i valori di cui si discute sono percepiti e tutelati nei diversi contesti culturali e normativi di riferimento cfr., S. E. Merry, *McGill Convocation Address: Legal Pluralism in Practice*, in *McGill Law Journal*, 2013, 59, 1, consultabile all'indirizzo: *http://lawjournal.mcgill.ca/userfiles/other/75931-Article_1_Merry.pdf*; con riferimento, invece, alla relatività del concetto di *privacy* cfr., L. A. Bygrave, *Privacy Protection in a Global Context — A Comparative Overview*, in *Scandinavian Studies in Law*, 2004, 47, 319 e ss., consultabile all'indirizzo: *http://folk.uio.no/lee/publications/Privacy%20in%20global%20context.pdf*, il quale evidenzia che: « *It is clear that levels of privacy across nations and cultures, and across broad historical periods, are in constant flux. Moreover, the ways in which human beings create, safeguard and enhance their respective states of privacy, and the extent to which they exhibit a desire for privacy, vary from culture to culture according to a complex array of factors* ».

danti, perché inerenti ai medesimi temi e basati sulla medesima logica argomentativa — sono stati fatti quindi oggetto di analisi dettagliata attraverso la lettura e la sistematizzazione degli stessi, che ha consentito di scartare i c.d. falsi-positivi.

In proposito, è necessario porre in luce come le decisioni esaminate raramente si riferiscano a trattamenti di dati personali realizzati mediante l'impiego delle più recenti applicazioni tecnologiche in materia di analisi dei dati, quali i sistemi di intelligenza artificiale o gli algoritmi di *machine learning*. La ragione di ciò può agevolmente ricondursi alla circostanza per la quale gli interessati non sono, ad oggi, ancora pienamente in grado di percepire i potenziali pregiudizi derivanti da tali impieghi; di conseguenza, i ricorsi sottoposti alle autorità garanti concernenti soluzioni di *big data analytics* ovvero dispositivi IoT [30] sono ancora poco numerosi.

A valle di questa disamina sono state individuate le pronunce ritenute più significative, laddove in maniera più evidente è emersa l'attenzione delle autorità garanti verso i diritti e le libertà fondamentali suscettibili di subire un pregiudizio dall'uso dei dati. Al riguardo, come si avrà modo di verificare, l'esame delle considerazioni espresse da parte delle autorità garanti ha consentito di individuare una certa uniformità di approccio, evidenziando come i principi nonché i diritti e le libertà riconosciuti in materia di diritti umani siano elementi comuni all'interno di questo *corpus* di decisioni. Tale omogeneità ha pertanto consentito di svolgere un'analisi per quanto possibile trasversale dei profili attinenti ai diritti presi in considerazione in occasione dei diversi interventi.

In proposito, è opportuno nondimeno evidenziare che in molte delle decisioni esaminate il riferimento ai diritti e alle libertà fondamentali coinvolti emerge sovente in maniera indiretta dalle osservazioni formulate dalle autorità garanti, sebbene non manchino ipotesi in cui tali profili sono espressamente richiamati. In tal senso, la tutela dei diritti e delle libertà fondamentali è spesso realizzata, mediante il ricorso ai tradizionali principi elaborati nell'ambito della disciplina sulla protezione dei dati personali, senza, dunque, un preciso richiamo al singolo diritto o alla particolare libertà destinati ad assumere rilevanza nel caso concreto [31]. Nel contesto degli interventi delle autorità garanti si

[30] L'IoT (*Internet of Things*), indica quella particolare architettura dell'informazione che consente l'interconnessione — mediante la rete Internet — di una pluralità di oggetti, fisici o virtuali, quali telecamere, elettrodomestici ovvero automobili. Con riferimento alla rete rappresentata dall'Internet degli oggetti, cfr., tra gli altri, Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, WP 223, del 16 settembre 2014.

[31] Con riferimento alle decisioni delle autorità garanti nazionali e alla posizione dalle medesime assunta rispetto ai principi espressi dalla Carta dei diritti fondamen-

rinviene, dunque, il ricorso ai generali principi — quali quello di finalità, di legittimità, di necessità, di trasparenza, di pertinenza e di non eccedenza — per tutelare in maniera criptica diritti fondamentali differenti da quello sui dati.

Nello specifico, è frequente l'impiego del principio di proporzionalità al fine di operare un bilanciamento dei diversi interessi coinvolti nel caso concreto. Nel valutare la legittimità di un determinato trattamento, le autorità garanti considerano, infatti, i diversi interessi in gioco e, dunque, da un lato le esigenze sottese ai trattamenti dei dati personali e, dall'altro lato, le diverse prerogative delle persone coinvolte, suscettibili di subire un pregiudizio dall'uso delle proprie informazioni [32]. La formulazione di tale giudizio si riduce, tuttavia, frequentemente, ad un'enunciazione assiomatica, ove la valutazione dei diversi interessi non risulta adeguatamente motivata nel contesto delle singole decisioni ed il perno della motivazione ruota sui menzionati principi generali, lasciando maggiormente in ombra il concreto bilanciamento sotteso alla decisione.

tali, cfr., M. G. Porcedda, *Use of the Charter of Fundamental Rights by National Data Protection Autorities and the EDPS*, Centre for Judicial Cooperation (CJC), Robert Schuman Centre for Advanced Studies, European University Institute, consultabile al seguente indirizzo: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3157786*.

[32] Cfr., *ex multis*, Garante per la protezione dei dati personali, 8 settembre 2016, n. 350, doc. web 5497522; Garante per la protezione dei dati personali, 4 giugno 2015, n. 345, doc. web n. 4211000, avente ad oggetto il controllo da parte del datore di lavoro di alcune comunicazioni della dipendente effettuate — sia nello svolgimento della propria attività di lavoro che al di fuori di essa — mediante l'utilizzo del software Skype installato sul computer aziendale usato dalla medesima. In quell'occasione il Garante ha evidenziato che: « (…) *il contenuto di comunicazioni di tipo elettronico e/o telematico scambiate dal dipendente nell'ambito del rapporto di lavoro sono assistite da garanzie di segretezza tutelate anche a livello costituzionale 'la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali'* (punto 5.2 lett. b)); *ciò comporta la necessità che l'eventuale trattamento dei dati riferiti a comunicazioni di posta elettronica o assimilabili, inviate e ricevute dal dipendente nello svolgimento dell'attività lavorativa, debba essere garantito da un elevato livello di tutela atto ad impedire, in un'ottica di bilanciamento con i contrapposti interessi del datore di lavoro e in attuazione dei principi di necessità, correttezza, pertinenza e non eccedenza, 'un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata'* »; Agencia Española de Protección de Datos, Expediente n. 01760/2017, riguardante l'installazione, da parte del datore di lavoro, di telecamere di sorveglianza nelle zone dedicate al relax dei dipendenti. In quell'occasione, il garante spagnolo ha osservato, in particolare, che: « *El tratamiento de datos realizado en el centro de trabajo por medio de cámaras de video vigilancia está exceptuado del consentimiento de los empleados, por la habilitación legal que le confiere al empresario el art. 20.3 del Estatuto de los Trabajadores, que comprende entre otras, la de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento del trabajador de sus obligaciones laborales. Esta facultad ha de producirse en todo caso, como es lógico, dentro del debido respeto a la dignidad del trabajador, como expresamente nos recuerda la normativa laboral.* (…). *La entidad denunciada como responsable del tratamiento, debe tener en cuenta la relación de proporcionalidad entre la finalidad perseguida y el modo en el que se tratan los datos, a fin de garantizar el cumplimiento de los principios de proporcionalidad y finalidad previstos por los apartados 1 y 2 del mencionado artículo 4 de la LOPD, siendo obligación del responsable del tratamiento adecuar el uso de los datos personales de modo que el impacto en los dere-*

5. *Segue*. L'impatto del trattamento sui diritti e le libertà delle persone fisiche nella giurisprudenza delle autorità garanti italiana e spagnola.

Nonostante le delineate criticità, che complicano la ricostruzione della *ratio* argomentativa delle pronunce esaminate, dall'esame delle decisioni emerge in termini generali l'attenzione delle autorità garanti per una pluralità di diritti e libertà che va al di là della mera tutela dei dati personali e della riservatezza. Nel valutare la legittimità di un determinato trattamento, le scelte adottate dalle autorità garanti paiono infatti tener conto dei possibili pregiudizi che possono derivare a danno di una varietà di diritti e libertà fondamentali quali, ad esempio, la libertà di autonomia e di autodeterminazione, l'identità individuale, la libertà da discriminazione, l'integrità fisica e la dignità degli interessati [33].

In tale contesto è proprio l'esigenza di tutelare l'autonomia e l'autodeterminazione degli interessati ad emergere in modo ricorrente nelle decisioni esaminate, considerata sotto diversi profili. In particolare, nel contesto delle singole decisioni tale libertà è stata declinata sia come libertà di scelta, di comportamento e di movimento, sia come libertà di autonomia informativa, e di libero esercizio libertà nell'esercizio della professione o, ancora, come libero e armonico sviluppo della persona.

La libertà di scelta, di movimento e di comportamento, e, in generale, la centralità dell'attenzione all'autonomia personale nel ragionamento delle autorità garanti, emerge poi tanto con riferimento al comportamento individuale quanto rispetto al contesto relazionale.

Nello specifico, la dimensione individuale di tale libertà è rinvenibile nell'ambito di quelle decisioni che hanno ad oggetto trattamenti caratterizzati dall'impiego di strumenti di videosorveglianza o di sistemi che consentono la localizzazione degli interessati (quali, ad esempio, i sistemi GPS ovvero la tecnologia

chos de los afectados sea el mínimo posible. (…) *En definitiva, aun cuando el artículo 20.3 del ET. faculta al empresario para adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, esta adopción debe tener en cuenta obligatoriamente los derechos específicos de los trabajadores respetando los derechos a la intimidad y el derecho fundamental a la protección de datos* »; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 368/2006. Tutti i provvedimenti e i documenti di indirizzo adottati dall'Autorità garante spagnola e richiamati nel presente lavoro sono consultabili sul sito Internet della medesima autorità:. *https://www.aepd.es/*. Come altresì evidenziato dalle autorità garanti, il tema del bilanciamento tra contrapposti interessi assume particolare rilevanza nell'ambito del rapporto di lavoro: da un lato, infatti, vi è l'esigenza del datore di lavoro alla tutela degli interessi aziendali, dall'altro lato, invece, è necessario considerare il diritto del lavoratore al rispetto della propria riservatezza e dignità. In proposito, cfr., G. Finocchiaro, *Limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro*, cit., 51 e ss.

[33] Cfr., le pronunce delle autorità garanti richiamate *infra*.

RFID) [34], nonché di strumenti per la misurazione del *rating* reputazionale [35].

In proposito, le autorità garanti hanno evidenziato [36] come tali sistemi siano suscettibili di condizionare i comportamenti e gli spostamenti dell'interessato. Ne consegue che, ogniqualvolta gli strumenti impiegati consentano — per loro natura o per le modalità con cui gli stessi vengono utilizzati — di dar luogo a forme di monitoraggio continuo e/o invasivo, gli stessi devono ritenersi tali da limitare le scelte degli interessati che, consapevoli

[34] Con riferimento all'impiego di strumenti che consentono il controllo dell'attività dei lavoratori cfr., tra le altre, Garante per la protezione dei dati personali, 28 giugno 2018, n. 396, doc. web n. 9023246; Garante per la protezione dei dati personali, 18 aprile 2018, n. 232, doc. web n. 9358266, ove il Garante, pur ammettendo il trattamento dei dati relativi alla localizzazione dei dipendenti, anche in considerazione della particolare natura dell'attività esercitata, ha tuttavia richiesto l'adozione di determinati accorgimenti al fine di evitare un'eccessiva attività di monitoraggio e, conseguentemente, il condizionamento degli interessati; Garante per la protezione dei dati personali, 8 settembre 2016, n. 350, doc. web n. 5497522, ove il Garante, chiamato a pronunciarsi sulla legittimità dell'impiego di un trattamento dei dati personali connesso all'installazione di un'applicazione sul dispositivo *smartphone* dei dipendenti — contenente una funzionalità di localizzazione geografica e preordinato alla rilevazione delle presenze —, ha evidenziato in particolare che: « *considerato che i dati personali relativi alla geolocalizzazione — riferiti alla 'posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico'* (…) *— devono essere trattati adottando particolari cautele e che i dispositivi smartphone sono, in considerazione delle normali potenzialità d'uso e dell'utilizzo comune degli stessi, destinati a 'seguire' la persona che li detiene indipendentemente dalla distinzione tra tempo di lavoro e tempo di non lavoro, tale trattamento presenta rischi specifici per la libertà, i diritti e la dignità del dipendente* » (le medesime considerazioni si rinvengono, altresì, in: Garante per la protezione dei dati personali, 11 settembre 2014, doc. web n. 3474069; Garante per la protezione dei dati personali, 9 ottobre 2014, doc. web. n. 3505371); Agencia Española de Protección de Datos, Expediente n. E/02689/2012: « *Cuando para el desarrollo de la función empresarial de control se utilizan las tecnologías de la información, las posibilidades de repercusión en los derechos del trabajador se multiplican y se manifiestan de muy diversos modos. Pueden citarse entre otros, los controles biométricos como la huella digital, la videovigilancia, los controles sobre el ordenador, -como las revisiones, el análisis o la monitorización remota, la indexación de la navegación por Internet, o la revisión y monitorización del correo electrónico y/o del uso de ordenadores-, o los controles sobre la ubicación física del trabajador mediante geolocalización. En la mayor parte de estos supuestos existen tratamientos de datos personales y, en consecuencia es necesario cumplir con los principios de protección de datos.* (…) *Por otro lado, el uso de tecnologías de la información multiplica las posibilidades de control empresarial y obliga a tener en cuenta el respeto a los derechos fundamentales de los trabajadores, a adoptar medidas de control que sean proporcionales y respeten su dignidad, su derecho a la protección de datos y su vida privada* ». Con riferimento, invece, agli strumenti di videosorveglianza e di localizzazione impiegati al di fuori del contesto lavorativo, cfr., *ex multis*, Garante per la protezione dei dati personali, 7 novembre 2013, n. 499, doc. web n. 2911484, ove la fattispecie sottoposta all'attenzione del Garante riguardava l'installazione, da parte di una società operante nel settore del noleggio a breve e medio termine di auto e veicoli commerciali, di un dispositivo multifunzione annoverabile tra i c.d. *event data recorder*, contenente, tra l'altro, sistemi di videosorveglianza e di geolocalizzazione. In quell'occasione, il Garante, pur ritenendo legittima l'acquisizione dei dati in funzione delle finalità perseguite, ha evidenziato come il loro impiego richieda particolari cautele al fine di garantire il rispetto « dei diritti e delle libertà fondamentali, nonché della dignità degli interessati », in tal modo dando atto, seppur implicitamente, dei gravi pregiudizi che possono derivare dall'impiego di tali strumenti, con riferimento, in particolare alla libertà di autodeterminazione degli interessati, ol-

dell'altrui controllo, potrebbero essere portati ad assumere il comportamento ritenuto maggiormente rispondente alle aspettative del sorvegliante [37].

Dalle osservazioni formulate dalle medesime autorità emerge, inoltre, come le conseguenze derivanti dai trattamenti dei dati siano suscettibili di atteggiarsi diversamente a seconda del contesto di riferimento ovvero delle concrete modalità di impiego degli strumenti finalizzati al trattamento. In questo senso, la potenziale limitazione dell'autonomia delle persone soggette al trattamento, derivante da forme di monitoraggio, assume particolare rilievo, ad esempio, nell'ambito del rapporto di lavoro, in ragione dello squilibrio di posizioni tra titolare del trattamento e interessato che caratterizza tale contesto [38].

Come anticipato, la possibilità riconosciuta al singolo di determinarsi autonomamente non si limita al piano individuale ma si manifesta, altresì, nel contesto relazionale. Nello specifico, la dimensione relazionale emerge in maniera piana in quelle decisioni aventi ad oggetto situazioni caratterizzate dallo scambio di informazioni da parte degli interessati, in occasione delle quali le autorità garanti hanno posto in luce come l'attività di sorveglianza delle comunicazioni sia suscettibile di condizionare il comportamento dell'interessato, con riferimento, in particolare, al contenuto delle medesime.

In questo senso vengono in considerazione sia quelle forme di

---

treché alla loro dignità; Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017. Con riferimento, invece, all'impiego dei sistemi di *Radio Frequency Identification* (RFID), cfr., Garante per la protezione dei dati personali, 9 marzo 2005, doc. web n. 1109493, *"Etichette intelligenti" (Rfid): il garante individua le garanzie per il loro uso*.

[35] Cfr., Garante per la protezione dei dati personali, 24 novembre 2016, n. 488, doc. web n. 5796783, in occasione della quale il Garante italiano ha evidenziato, come nelle ipotesi in cui tali strumenti abbiano ad oggetto la raccolta e la successiva pubblicazione di informazioni "delicate" relative agli interessati — quali, ad esempio, quelle riguardanti i certificati del casellario giudiziale, i certificati di regolarità fiscale, la presenza di eventuali denunce o querele nei confronti dei medesimi, ovvero lo svolgimento di attività di volontariato — gli stessi siano in grado di incidere significativamente, tra l'altro, sulla libertà di autodeterminazione di questi ultimi, nella misura in cui sono in grado di influenzarne le scelte e i comportamenti al fine di evitare eventuali giudizi negativi.

[36] Cfr., le decisioni richiamate *supra*, *sub* note 34 e 35.

[37] Si tratta del c.d. *chilling effect* derivante, in tal caso, da forme di monitoraggio continuo e/o invasivo. Il *chilling effect* è un concetto che viene impiegato per indicare il risultato di un certo evento in grado di dar luogo ad un'azione deterrente verso un dato comportamento. Con riferimento al *chilling effect* che l'attività di sorveglianza può realizzare rispetto al comportamento dell'interessato, cfr., tra gli altri, R. Clarke, *The regulation of civilian drones' impacts on behavioural privacy*, in *Comp. Law & Sec. Rev.*, 2014, 30, 3, 287 s.; P. P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, in *Washington Univ. Law Rev.*, 1999, 77, 2, 473 e ss.; J. W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, in *Berkeley Tech. Law Journ.*, 2016, 31, 1, 117 e ss.; S. J. Daniel, *A Taxonomy of Privacy*, in *University of Pennsylvania Law. Rev.*, 2006, 154, 3, 477 e ss.

[38] In proposito, cfr., *ex multis*, le decisioni aventi ad oggetto trattamenti effettuati nel contesto lavorativo richiamate *supra*, *sub* nt. 34, nonché, tra le tante, Garante per la protezione dei dati personali, 24 febbraio 2010, doc. web n. 1705070.

comunicazione tradizionalmente intese — rientrando in tale categoria tutte quelle forme di comunicazione di tipo *one-to-one*, che si svolgono, ad esempio, mediante lo scambio di email ovvero per il tramite di conversazioni telefoniche [39] —, sia quelle forme di comunicazione che avvengono in ambienti condivisi mediante piattaforme che consentono interazioni multiple, quali, ad esempio, quelle realizzate per il tramite dei *social networks* [40].

Nel contesto delle decisioni prese in esame, l'ampia nozione di tutela della libertà di scelta si concretizza, poi, anche in termini di autonomia informativa [41] degli interessati. È questo il caso, ad esempio, di quei servizi la cui fruibilità da parte degli utenti venga subordinata al previo consenso al trattamento per finalità di *marketing* [42]. Al riguardo, nel valutare negativamente la legittimità di tali trattamenti, è stato posto in luce, in particolare, come queste pratiche limitino la libertà degli interessati nell'assumere le

[39] Cfr., *ex multis*, Garante per la protezione dei dati personali, 1 febbraio 2018, doc. web n. 8159221, ove il Garante, chiamato a pronunciarsi sulla legittimità di un trattamento di dati personali effettuato dal datore di lavoro mediante il controllo del contenuto delle email, anche di natura privata, scambiate dal lavoratore, ha evidenziato che: « *il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità*. (…) *Tanto più che l'assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. (…) L'interesse del titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività, pertanto, deve essere contemperato con la legittima aspettativa di riservatezza sulla corrispondenza da parte dei dipendenti nonché dei terzi* »; Garante per la protezione dei dati personali, 22 dicembre 2016, n. 547, doc. web n. 5958296; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013.

[40] Al riguardo, può altresì richiamarsi quanto osservato dalle Autorità di protezione dei dati con riferimento alle informazioni disponibili sui *social network*: Garante per la protezione dei dati personali, doc. web n. 1567124.

[41] Con riferimento al diritto all'autodeterminazione informativa, v., *ex multis*, la rilevante pronuncia della Corte Costituzionale tedesca: Bundesverfassungsgericht, 15 dicembre 1983, in *Entscheidungen des Bundesverfassungsgerichts*, 1984, 65, 1 ss.; in dottrina, cfr., G. Sartor, *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del « Datenschutz »*, in *Inf. dir.*, 1986, 3, 95 e ss., a parere del quale il diritto all'autodeterminazione informativa rappresenterebbe un « *diritto di libertà* », diretto a garantire l'autonoma determinazione del singolo in merito alla circolazione delle informazioni che lo riguardano; E. Fialova, *Data Portability and Informational Self-Determination*, in *Masaryk U. J.L. & Tech.*, 8, 2014, 47 e ss.; E. J. Eberle, *The Right to Information Self-Determination*, in *Utah L. Rev.*, 2002, 695, 4, 968 e ss.

[42] Con riferimento al trattamento dei dati personali nel contesto delle comunicazioni effettuate per finalità di *marketing*, cfr., altresì, le disposizioni contenute nella "*Proposta di regolamento europeo per la tutela dei dati nel contesto della fornitura e della fruizione di servizi di comunicazione elettronica*" presentata dalla Commissione europea nel gennaio 2017 al Consiglio. Il Regolamento, una volta adottato, andrai a sostituire la Direttiva *ePrivacy* 2002/58/CE: *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)*, consultabile all'indirizzo: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010*.

proprie scelte e le proprie determinazioni in merito all'utilizzo dei dati [43].

Ancora, la libertà di autonomia e autodeterminazione è stata intesa, altresì, quale libertà diretta a tutelare l'autonomia degli interessati nell'esercizio della propria professione. Questo è emerso, ad esempio, con riferimento ai trattamenti effettuati per il tramite dell'installazione di sistemi di videosorveglianza all'interno delle aule didattiche di un asilo nido, in grado di consentire ai genitori un controllo a distanza dei propri figli. Nello specifico, con riferimento a tali trattamenti è stata posta in luce l'esigenza di garantire la libertà di scelta dei metodi educativi e d'insegnamento dei docenti coinvolti nel trattamento [44].

Infine, la libertà di autonomia e autodeterminazione è stata anche presa in considerazione anche con riferimento alla necessità di assicurare adeguata tutela al libero e armonico sviluppo delle persone soggette al trattamento. In questo senso vengono in considerazione, ad esempio, le attività del datore di lavoro dirette al controllo delle comunicazioni elettroniche scambiate dai propri dipendenti — sia per finalità connesse al contesto lavorativo sia per motivi estranei allo stesso — ovvero della navigazione Internet da parte dei medesimi [45]. Nello specifico, nell'ambito delle decisioni esaminate è stato evidenziato come il controllo delle comunicazioni, così come del comportamento *online* [46], sia suscettibile di dar luogo a gravi forme di condizionamento, in grado di incidere, altresì, sui rapporti dell'interessato con gli altri consociati [47].

Al di fuori del contesto delle comunicazioni, la tutela del libero e armonico sviluppo degli interessati, quale aspetto della libertà di

---

[43] Garante per la protezione dei dati personali, 27 ottobre 2016, 2016 n. 439, doc. web n. 5687770, ove si evidenzia che: « la capacità di autodeterminazione degli utenti (e quindi la libertà del consenso che sono chiamati a manifestare) non è assicurata quando si assoggetta, (…), la fruizione delle prestazioni dedotte nel contratto alla contestuale autorizzazione a trattare i dati conferiti per il medesimo servizio per una finalità diversa, qual è quella promozionale e pubblicitaria »; in argomento, cfr., altresì, Garante per la protezione dei dati personali, 13 maggio 2015 n. 291, doc. web n. 4337465; Garante per la protezione dei dati personali, 24 novembre 2016, n. 488, *cit*.

[44] Garante per la protezione dei dati personali, 8 maggio 2013, n. 230, doc. web n. 2433401.

[45] Garante per la protezione dei dati personali, 4 giugno 2015, n. 345, cit. (v. *supra* nota 32); Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0464/2013.

[46] In generale, con riferimento al controllo del datore di lavoro mediante *social network*, cfr., tra gli altri, M. Forlivesi, *Il controllo della vita del lavoratore attraverso i* social network, in P. Tullini (a cura di), Web *e lavoro. Profili evolutivi e di tutela*, *cit.*, 37 e ss.

[47] In proposito va osservato come anche l'ambiente lavorativo rappresenti senz'altro un contesto sociale nel quale il lavoratore è in grado di sviluppare la propria personalità, ai sensi dell'art. 2 Cost. In questo senso, dunque, la tutela della persona del lavoratore non si concretizza nella mera dimensione individuale, ma anche in quella relazionale, mediante il riconoscimento della possibilità di stabilire relazioni con altri. In questo senso, cfr., C. Colapietro, T*utela della dignità e della riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Gior-*

autonomia e autodeterminazione ai medesimi riconosciuta, è emersa, invece, sia con riferimento all'ipotesi di diffusione di dati riguardanti minori vittime di violenza sessuale da parte degli organi di informazione [48] sia rispetto all'installazione da parte di un hotel di sistemi di videosorveglianza diretti a monitorare le aree dedicate al relax dei clienti [49]. Al riguardo, le autorità garanti hanno in particolare evidenziato come tali attività siano in grado di ripercuotersi sulle relazioni sociali dell'interessato e, in generale, sulla sua vita privata.

L'interesse in esame è stato poi preso in considerazione anche con riferimento all'ipotesi, sopra richiamata, dell'installazione di sistemi di videosorveglianza all'interno di un asilo nido [50], rispetto alla quale, oltre all'esigenza di salvaguardare l'autonomia dell'attività professionale dei docenti, possono invero emergere profili inerenti alla tutela del libero e armonico sviluppo dei minori.

Un ulteriore importante nucleo di interessi e libertà oggetto di particolare attenzione da parte delle autorità nazionali è riconducibile alla sfera del diritto all'identità dell'interessato [51], la quale può subire un pregiudizio, ad esempio, a fronte di tratta-

nale dir. lav. rel. ind., 2017, n. 3, 450; in giurisprudenza, cfr., *ex multis*, Corte eur. dir. uomo, 16 dicembre 1992, *Niemietz v. Germany*, *Application no. 13710/88*, consultabile all'indirizzo: *http://adapt.it/adapt-indice-a-z/wp-content/uploads/2016/01/Niemietz_Germany.pdf*, ove si legge in particolare che: « *The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'. However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world* »; Garante per la protezione dei dati personali, *Linee guida per posta elettronica e Internet*, 1 marzo 2007, n. 13, doc. web n. 1387522: « *Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato)* ».

[48] Garante per la protezione dei dati personali, 10 luglio 2008, doc. web n. 1536583.

[49] Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017.

[50] Garante per la protezione dei dati personali, 8 maggio 2013, n. 230, cit.

[51] Il riferimento al diritto all'identità dell'interessato emerge in questo contesto al fine di tutelare quell'insieme di informazioni che identificano il singolo individuo e che consentono di distinguerlo dagli altri consociati. Con riferimento alle diverse accezioni della nozione "identità personale", cfr., V. Zeno-Zencovich, voce *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993, 294; G. Resta, *Dignità, Persone, Mercati*, Torino, 2014, 324 e ss.

menti diretti a raccogliere dati univoci della persona. Nello specifico, si tratta, di tutti quegli strumenti in grado di individuare e raccogliere informazioni strettamente inerenti all'identità, quali i dati biometrici, che sempre più spesso vengono impiegati (sia nell'ambito del rapporto di lavoro che al di fuori dello stesso) per regolare l'accesso a determinati spazi e servizi.

L'esigenza di porre attenzione al trattamento dei dati relativi all'identità dell'interessato deriva, in particolare, dalla constatazione per la quale tali informazioni sono strettamente inerenti alla persona e, specie nel caso di dati biometrici o genetici, non sono facilmente modificabili o immodificabili. Un eventuale uso abusivo di tali dati è suscettibile di arrecare conseguenze pregiudizievoli di rilievo, come quelle derivanti dall'eventuale furto d'identità [52].

Le decisioni esaminate hanno inoltre consentito di individuare nel diritto alla non discriminazione un ulteriore elemento di rilievo che informa le linee argomentative delle autorità garanti. In particolare, dall'esame delle decisioni è emerso come l'esigenza di tutelare il singolo da eventuali forme di discriminazione possa venire in considerazione nell'ambito di una pluralità di contesti e in relazione a diverse tipologie di trattamenti [53].

In proposito, può ad esempio richiamarsi una pronuncia del Garante italiano avente ad oggetto un trattamento di dati sensibili (in particolare, di quelli idonei a rivelare l'origine etnica o razziale, le convinzioni religiose, lo stato di salute ovvero l'orientamento sessuale), realizzato da parte di un'agenzia di interme-

---

[52] Garante per la protezione dei dati personali, 18 giugno 2015, n. 360, doc. web n. 4170232, avente ad oggetto l'impiego di un particolare strumento biometrico basato su un sistema di riconoscimento facciale (c.d. *face recognition*) da parte di una società operante nel settore dei viaggi da crociera. L'impiego di tale sistema era finalizzato ad agevolare i clienti nell'individuazione — a scopo di acquisto — delle fotografie che li ritraevano durante la loro permanenza a bordo della nave. In quell'occasione, dunque, il Garante ha evidenziato l'esigenza di porre in essere determinate cautele nell'utilizzo di tali strumenti, riconoscendo — seppur implicitamente — che gli stessi, essendo idonei a registrare dati univoci e immutabili degli interessati, sono suscettibili di impieghi abusivi ed illeciti da parte di terzi estranei, con conseguente pregiudizio per l'identità dell'interessato; Garante per la protezione dei dati personali, 15 giugno 2006, doc. web. n. 1306098, ove si evidenzia che: « *l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è in linea di principio lecito. Tali dati, per loro peculiare natura, richiedono l'adozione di elevate cautele al fine di prevenire possibili pregiudizi ai danni degli interessati, con particolare riguardo a condotte illecite che determinano l'abusiva 'ricostruzione' dell'impronta partendo dal template e la sua ulteriore 'utilizzazione' all'insaputa degli stessi* »; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0392/2011.

[53] Con riferimento al rischio di discriminazione che può derivare dal trattamento dei dati personali nell'attuale contesto tecnologico e informatico, oltre ai contributi richiamati *supra*, *sub* nota 8, v., *ex multis*, S. P. Gangadharan, V. Eubanks, S. Barocas (eds.), *Data discrimination: collected essays*, *Open Tech. Inst.*, *New America*, 2014, 1 e ss., disponibile all'indirizzo: *https://www.newamerica.org/oti/policy-papers/data-and-discrimination/*; B. Custers, T. Calders, B. Schermer, T. Zarsky (eds.), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Springer, 2013.

diazione immobiliare al solo scopo di soddisfare determinate esigenze di natura discriminatoria manifestate dai proprietari degli immobili [54].

L'esigenza di tutelare l'interessato contro eventuali forme di discriminazione è emersa, inoltre, con riferimento ai trattamenti dei dati personali effettuati nell'ambito del rapporto di lavoro. È il caso, ad esempio, delle informazioni richieste da parte del datore di lavoro non necessarie allo svolgimento della prestazione lavorativa, quali quelle relative alle opinioni politiche e sindacali dei propri dipendenti [55].

Ancora, nell'ambito delle decisioni esaminate è stata posta in luce l'esigenza di tutelare l'integrità fisica dell'interessato, suscettibile di subire un pregiudizio in occasione di determinati trattamenti. In questo ambito vengono in considerazione tutti quegli strumenti diretti alla raccolta di informazioni inerenti all'interessato suscettibili di tradursi in forme invasive della sfera fisica dello stesso, come l'impiego di sistemi RFID mediante l'uso di microchip sottocutanei in grado di incorporare informazioni personali relative ai portatori (quali, ad esempio, i dati identificativi, il numero di carta di credito o le informazioni sanitarie). L'autorità garante spagnola, chiamata a pronunciarsi sulla legittimità di tale trattamento, ha posto l'accento sull'elevato grado di invasività di tali strumenti, siccome capaci di incidere significativamente sulla sfera fisica e personale dell'interessato. Per queste ragioni, l'autorità ne ha limitato l'impiego alle ipotesi in cui non sia possibile il ricorso a strumenti meno invasivi che consentano il raggiungimento delle medesime finalità [56].

Infine, un interesse preminente nelle carte dei diritti fondamentali emerso in modo costante nelle decisioni delle autorità garanti è la tutela della dignità dell'interessato. In particolare, dalle diverse pronunce esaminate emerge come la dignità personale possa manifestarsi in diverse forme e in diversi contesti, i quali possono essere caratterizzati o meno da particolari forme di squilibrio di poteri.

Al riguardo, possono richiamarsi, ad esempio, i casi dei trattamenti di dati posti in essere mediante l'impiego di strumenti biometrici [57], di quelli in grado di dar luogo a forme di pubblicità

[54] Garante per la protezione dei dati personali, 11 gennaio 2007, doc. web n. 1381620.

[55] In questo senso, cfr., tra le altre, Garante per la protezione dei dati personali, 1 luglio 1998, doc. web n. 42332.

[56] Cfr., Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0292/2010. Le medesime preoccupazioni in merito all'installazione di microprocessori sottocutanei sono state espresse dal Garante italiano: cfr., Garante per la protezione dei dati personali, 9 marzo 2005, doc. web n. 1109493, *cit*.

[57] Al riguardo, cfr., *ex multis*, Garante per la protezione dei dati personali, 1 agosto 2013, n. 384, doc. web n. 2578547, ove, con riferimento ai sistemi di riconoscimento biometrico impiegati sui lavoratori allo scopo di rilevarne la presenza, si evi-

della situazione patrimoniale [58] ovvero idonei a rivelare a terzi le posizioni debitorie dell'interessato [59]. Nello specifico, le autorità garanti hanno posto in luce come tali trattamenti siano anche suscettibili di dar luogo, a seconda dei casi, a conseguenze di carattere denigratorio o lesive dell'onore personale e/o professionale.

Con riferimento ai trattamenti suscettibili di ledere la dignità degli interessati, possono inoltre richiamarsi gli strumenti per la misurazione del *rating* reputazionale, come visto oggetto di attenzione da parte dell'autorità garante italiana. Nello specifico, il Garante ha espresso numerose preoccupazioni rispetto alla legittimità di tali strumenti, i quali, oltre ad incidere sulla riservatezza e la libertà di autodeterminazione dei soggetti censiti, sono suscettibili di ripercuotersi significativamente sulla rappresentazione economica e sociale degli stessi [60].

Ancora, dalle decisioni esaminate è emerso come esigenze di tutela della dignità dell'interessato possono venire in considerazione, altresì, in presenza di trattamenti di dati personali che si traducano in forme di monitoraggio continuo. In proposito, può richiamarsi una decisione del garante italiano avente ad oggetto l'impiego da parte di una residenza sanitaria-assistenziale di dispositivi elettronici (nella specie, braccialetti o cavigliere), idonei a consentire di individuare la posizione del paziente all'in-

denzia che: « *Il titolare del trattamento* (…), *allo scopo di verificare il puntuale rispetto dell'orario di lavoro ben può disporre di altri (più 'ordinari') sistemi, meno invasivi della sfera personale nonché della libertà individuale del lavoratore, che non ne coinvolgano la dimensione corporale aspetti, questi, costitutivi della dignità personale* »; Garante per la protezione dei dati personali, 21 luglio 2005, doc. web n. 1150679; Garante per la protezione dei dati personali, 11 dicembre 2000, doc. web n. 30903; Garante per la protezione dei dati personali, 15 giugno 2006, n. 1306098; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 368/2006, cit.; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0065/2015; Agencia Española de Protección de Datos, Gabinete Jurídico, Informe 0392/2011.

[58] Cfr., Garante per la protezione dei dati personali, 8 giugno 1999, doc. web n. 40369.

[59] Cfr., Garante per la protezione dei dati personali, 28 maggio 2015, n. 319, doc. web n. 4131145, avente ad oggetto lo svolgimento da parte di un servizio di *Pay-Tv* di attività finalizzate al recupero stragiudiziale dei crediti, mediante l'invio, ai propri clienti, di comunicazioni visualizzate automaticamente sullo schermo del televisore. In quell'occasione il Garante ha invero evidenziato come tali attività siano suscettibili di ledere la sfera personale e la dignità dell'interessato, stante il loro carattere invasivo e la possibilità che esse offrono di far conoscere a terzi la presenza di posizioni debitorie a carico del destinatario.

[60] In proposito, significative sono le osservazioni espresse dal Presidente del Garante per la protezione dei dati personali, il quale ha evidenziato in particolare che: « *l'idea di affidare la 'recensione' di una persona ad un algoritmo rischia di aprire davvero una deriva assai pericolosa. (…) È evidente che la reputazione degli individui che si vorrebbe quantificare per attribuire punteggi di affidabilità è strettamente legata alla persona considerata nella sua proiezione sociale e risulta intimamente connessa con la dignità, elemento cardine della disciplina in materia di protezione dei dati personali* », cfr., A. Soro, *La reputazione* online *tra principi di dignità e diritto all'oblio digitale*, in *L'Huffington Post*, 6 ottobre 2015, consultabile all'indirizzo: *https://www.huffingtonpost.it/antonello-soro/la-reputazione-online-tra-principi-di-dignita-e-diritto-alloblio-digitale_b_8250828.html*.

terno della struttura [61]. Il garante, pur ammettendo la legittimità di tale trattamento — anche in considerazione delle finalità di tutela perseguite, nonché delle concrete modalità di registrazione dei dati — ha evidenziato una serie di accorgimenti necessari al fine di tutelare la dignità dei pazienti, siccome suscettibile di subire gravi pregiudizi a fronte di forme di monitoraggio invasive.

inoltre, sono stati ritenuti particolarmente lesivi per la dignità anche tutti quegli strumenti in grado di acquisire informazioni che coinvolgono la sfera intima delle persone interessate dal trattamento. È il caso, ad esempio, dell'installazione di sistemi di videosorveglianza all'interno degli spogliatoi di una piscina in grado di raccogliere le immagini degli utenti mentre gli stessi si cambiavano [62], o dell'ipotesi di un trattamento caratterizzato dall'impiego, da parte del datore di lavoro, di tagliandi per consentire l'allontanamento dei dipendenti per necessità fisiologiche [63]. Ancora, con riferimento ai trattamenti ritenuti suscettibili di incidere negativamente sulla sfera intima dell'interessato viene altresì in considerazione la decisione del garante spagnolo sopra citata, avente ad oggetto l'installazione da parte di un hotel di sistemi di videosorveglianza nelle aree dedicate al relax dei clienti e, in particolare, nell'area della piscina e del giardino in cui erano collocati i lettini per prendere il sole [64].

Rispetto ai trattamenti ritenuti pregiudiziali per la dignità dell'interessato può infine richiamarsi una decisione del garante italiano concernente la legittimità delle informazioni raccolte da parte del datore di lavoro in occasione di una procedura di selezione del personale [65]. Nella specie, i quesiti sottoposti ai candidati concernevano fatti del tutto irrilevanti ai fini dell'accertamento dell'attitudine professionale dei lavoratori, essendo rivolti ad acquisire elementi informativi attinenti alla sfera affettiva, sessuale, sanitaria, nonché alle abitudini personali o ad altre vicende individuali dell'interessato.

In quell'occasione il garante ha evidenziato, in particolare, come l'acquisizione di informazioni dettagliate in merito alla sfera

---

[61] Cfr., Garante per la protezione dei dati personali, 25 gennaio 2018, doc. web n. 7810766.

[62] Cfr., Garante per la protezione dei dati personali, 8 marzo 2007, doc. web n. 1391803.

[63] Cfr., Garante per la protezione dei dati personali, 24 febbraio 2010, doc. web n. 1705070, cit., ove si è osservato in particolare che: « *l'acquisizione, a mezzo compilazione dei tagliandi scritti, di dati personali relativi alle necessità 'fisiologiche' dei lavoratori risulta contraria all'art. 2 del Codice, il quale prevede che il trattamento dei dati personali debba essere effettuato nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati; ciò soprattutto in considerazione del potenziale condizionamento (finanche in termini di mortificazione personale) che tale trattamento può ingenerare nei lavoratori in ordine alla propria libertà di movimento per l'espletamento dei relativi bisogni fisiologici* ».

[64] V., Agencia Española de Protección de Datos, Procedimiento n. A/00109/2017, cit.

[65] Cfr., Garante per la protezione dei dati personali, 21 luglio 2011, doc. web. n. 1825852.

privata dei partecipanti ad una procedura selettiva — come detto, non significative rispetto alla prestazione lavorativa — rappresentasse un'ingiustificata intrusione nella sfera intima, suscettibile di determinare turbamenti nell'animo, fino ad incidere negativamente sulla dignità personale e sociale dei medesimi.

6. Osservazioni conclusive.

I nuovi scenari offerti nel campo dell'informatica e della tecnologia costringono ad una riflessione più estesa delle implicazioni derivanti dall'uso dei dati personali.

Circostanze quali l'ampiezza e la natura delle informazioni oggetto del trattamento, il contesto di riferimento ovvero gli strumenti impiegati ai fini della raccolta dei dati, sono invero suscettibili di incidere in diverso modo sui diritti e le libertà degli individui, nonché sui valori etici e sociali tradizionalmente condivisi.

In questo contesto, dunque, è evidente come le nozioni di *privacy* e di *data protection* non offrano un'adeguata risposta a tutti gli effetti negativi che possono derivare dalle moderne tecnologie *data-intensive*. Da qui l'esigenza di una valutazione più ampia dei rischi che possono derivare dall'uso dei dati, in grado di ricomprendere tutti i diritti umani e le libertà fondamentali degli interessati suscettibili di venire in considerazione nel caso concreto.

Al riguardo, sebbene sia possibile rinvenire — sia a livello normativo che dottrinale — numerose istanze in merito alla necessità di guardare ai più ampi rischi inerenti ai diritti fondamentali ed ai profili etico-sociali dell'uso dei dati, i modelli di analisi e gestione del rischio in uso e recentemente elaborati dalle autorità garanti risultano ancora incentrati sulla tutela della qualità e della sicurezza delle informazioni.

L'esame dell'elaborazione giurisprudenziale delle autorità garanti italiana e spagnola ha quindi consentito di mettere in luce l'emergere di una pluralità di diritti e libertà che possono essere coinvolti nel contesto di un determinato trattamento, ben al di là della mera dimensione incentrata su qualità e modalità di trattamento del dato. Tali diritti e libertà dovranno pertanto trovare spazio nell'articolazione di un modello di *risk assessment* in grado di meglio rispondere alle potenziali criticità dell'uso delle informazioni nella moderna società digitale.

Emerge, dunque, la necessità che la tutela di questa più ampia gamma di diritti e libertà venga resa maggiormente esplicita e vengano elaborati nuovi modelli operativi volti a rendere l'utilizzo dei dati personali maggiormente conforme alle aspettative sociali, sia in termini di tutela dei diversi diritti fondamentali potenzialmente pregiudicati dal trattamento, che di considerazione delle

diverse istanze etiche e sociali che possono venire in esame in occasione di particolari trattamenti.

Appare pertanto evidente l'esigenza di adottare un approccio più ampio nella valutazione del rischio nel contesto della tutela dei dati personali e l'opportunità di elaborare differenti modelli di analisi e gestione dei rischi in grado di far fronte alle nuove e più ampie sfide derivanti dall'uso delle informazioni.

Abstract

The current technological and social scenario raises new issues with regard to the risks related to the use of data. This suggests to develop broader impact assessment models which consider all the human rights and fundamental freedoms likely to suffer prejudice in the context of a personal data processing.

In order to outline a general paradigm of values to be used as a benchmark in the assessment process, the paper focuses on the approaches adopted by the Italian and the Spanish data protection authorities, to highlight the driving interests underpinning their decisions.