ATTI PARLAMENTARI

XVIII LEGISLATURA

CAMERA DEI DEPUTATI

Doc. **CXXXVI**
n. **2**

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 2019)

(Articolo 154, comma 1, lettera e*), del codice di cui al decreto legislativo 30 giugno 2003, n. 196)*

Presentata dal Presidente del Garante per la protezione dei dati personali

(SORO)

Trasmessa alla Presidenza il 30 giugno 2020

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Protezione dati, emergenza, democrazia

Discorso del Presidente

Antonello Soro

Relazione2019

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
tel. 06 696771
email: protocollo@gpdp.it
www.garanteprivacy.it

Relazione2019

Discorso del Presidente

Antonello Soro

Roma, 23 giugno 2020

PAGINA BIANCA

1. Corpo, tecnica, libertà

Signor Presidente della Camera, Autorità, Signore e Signori,

un anno fa abbiamo presentato la relazione della nostra attività come conclusiva del mandato. Lo stallo nelle procedure di nomina, dovuto alla crisi di governo prima, all'emergenza sanitaria poi, ha prorogato sinora la nostra attività, non senza alcune difficoltà, dovute soprattutto all'incerto orizzonte di volta in volta prefigurato, con rinvii brevi del voto e ai limiti intrinseci del regime di ordinaria amministrazione, solo recentemente rimossi con l'intervento del legislatore.

Ciononostante, la nostra attività è stata sempre svolta con il massimo dell'impegno e della responsabilità, nella consapevolezza di dover garantire, senza soluzioni di continuità né affievolimenti sia pure momentanei, un diritto di libertà che, anche e soprattutto nel contesto emergenziale, si è dimostrato ancora più determinante. Un diritto inquieto, perché in costante evoluzione e mai tiranno, perché capace di porsi sempre in equilibrio con gli interessi giuridici che di volta in volta vengano in rilievo.

Ma la pandemia ha segnato - come in molti altri campi - un punto di non ritorno: il momento fondativo di una nuova consapevolezza.

Se fino a pochi mesi fa, nell'epoca più tecnicamente evoluta della storia umana, un timore diffuso era quello - forse ancestrale ma costantemente rinnovato - di una vera e propria sostituzione dell'uomo da parte delle macchine, oggi la paura si è materializzata nella concretezza del corpo, violato dalla malattia.

Questa rinnovata scoperta del naturale, del corporeo, del materiale, è servita, in un certo senso, a ricordarci come persino il progresso più avanzato, l'innovazione più audace - che paradossalmente l'emergenza ha appunto promosso - abbiano un fondamento umano, con cui dobbiamo fare i conti.

Ed è bene che da questa consapevolezza nasca un approccio diverso al rapporto tra uomo e tecnica, che sappia fare tesoro di tutto ciò che abbiamo vissuto, nel bene e nel male, in questi mesi.

La misura di prevenzione sanitaria più antica, ovvero la "quarantena" - che incide sulla concretezza del vivere quotidiano - si è affiancata al ricorso all'intelligenza artificiale negli studi epidemiologici e agli algoritmi quale ausilio diagnostico.

E le distanze fisiche imposte come misura, appunto la più antica, di contenimento dei contagi sono state colmate, paradossalmente, dalla prossimità offerta dalla tecnologia, capace di annullare gli spazi interposti tra i corpi e di ricostituire, nella dimensione digitale, quelle piazze svuotate nel reale.

Le distanze fisiche non sono divenute sociali grazie alla realizzazione, su innumerevoli piattaforme, di sale riunioni in cui lavorare senza rinunciare al confronto o classi dove formare ragazzi da remoto. Rispetto a tutte queste fattispecie abbiamo indicato - con strumenti agili quali linee guida e FAQ - cautele e condizioni per valorizzare al massimo l'uso della tecnologia salvaguardando l'autodeterminazione dei lavoratori, la libertà di insegnamento, la riservatezza dei minori.

Anche rispetto alla celebrazione da remoto di un processo, quale quello penale, strettamente ancorato al principio di oralità, al contraddittorio costante e alla dialettica d'aula, abbiamo segnalato l'esigenza di rafforzare le garanzie di sicurezza dei dati, delicatissimi, affidati ai canali telematici, per smaterializzare davvero - si è detto - le carte, non le persone.

Un contributo analogo ci è stato richiesto in ordine alla giustizia amministrativa, rispetto alla quale abbiamo suggerito anche un'interpretazione adeguatrice della vigente disciplina sulla pubblicità dei provvedimenti giurisdizionali.

La tecnica si è così prestata tanto alla libera esplicazione quanto al controllo della persona, esorcizzando anche la percezione di fragilità, ricostruendo legami e relazioni in un altrove divenuto, ormai, imprescindibile.

Ma come abbiamo rimosso, per decenni e anche più, la nostra vulnerabilità

fisica, ora rischiamo di ignorare quella, non meno insidiosa, del nostro io digitale.

La traslazione, mai così totalizzante, della nostra esistenza individuale e collettiva nella dimensione immateriale del web, espone infatti ciascuno di noi - in primo luogo attraverso i propri dati - alle sottili ma pervasive minacce di una realtà, quale quella digitale, tanto straordinaria quanto poco presidiata.

2. Diritti in emergenza

L'inattesa accelerazione impressa dalla pandemia alla transizione digitale impone oggi di ripensare, con altrettanta tempestività, il nostro modo di concepire questa nuova dimensione della vita, ormai sempre più indistinguibile da quella tradizionale, le cui coordinate godono tuttavia della solidità assicurata da prassi radicate.

L'epidemia ha profondamente mutato, infatti, l'allocazione dei poteri e le loro reciproche relazioni, non solo riarticolando l'equilibrio tra centro e periferia, politica e tecnocrazia, normazione e amministrazione, ma anche tracciando nuove coordinate del rapporto della nostra vita con il digitale e rendendone più urgente l'esigenza regolatoria, anche sotto il profilo della sostenibilità di sempre più incisivi poteri privati.

La devoluzione alla dimensione immateriale di pressoché tutte le nostre attività non è un processo neutro, ma comporta, se non assistito da adeguate garanzie, l'esposizione a inattese vulnerabilità in termini non solo di sicurezza informatica ma anche di soggezione a ingerenze e controlli spesso più insidiosi, perché meno percettibili di quelli tradizionali.

Particolarmente significativo è il contesto lavorativo, rispetto al quale abbiamo inteso fornire specifici chiarimenti anche in ordine alle attività di prevenzione e, più in generale, all'estensione dei poteri datoriali.

Il diffuso ricorso allo *smartworking* - generalmente necessitato e improvvisato - ha poi catapultato una quota significativa della popolazione in una

dimensione delle cui implicazioni non sempre si ha piena consapevolezza e di cui va impedito ogni uso improprio.

Potendo favorire una nuova articolazione dei processi produttivi in grado di accrescere efficienza e flessibilità, lo *smartworking* potrebbe ragionevolmente divenire una forma diffusa, effettivamente alternativa, di organizzazione del lavoro.

Per questa ragione andranno seriamente affrontati e risolti tutti i problemi emersi in questi mesi: dalle dotazioni strumentali alla garanzia di connettività, alla sicurezza delle piattaforme, all'effettività del diritto alla disconnessione, senza cui si rischia di vanificare la necessaria distinzione tra spazi di vita privata e attività lavorativa: annullando così alcune tra le più antiche conquiste raggiunte per il lavoro tradizionale.

Il ricorso intensivo alle nuove tecnologie per rendere la prestazione lavorativa non deve rappresentare l'occasione per il monitoraggio sistematico e ubiquitario del lavoratore, ma deve avvenire nel pieno rispetto delle garanzie sancite dallo Statuto a tutela dell'autodeterminazione, che presuppone anzitutto un'adeguata formazione e informazione del lavoratore.

Va, in particolare, inteso in modo rigoroso - lo abbiamo ricordato anche in sede parlamentare - il vincolo finalistico all'attività lavorativa che, rispetto ai controlli mediante strumenti utilizzati per rendere la prestazione, legittima l'esenzione dalla procedura concertativa o autorizzativa.

Per garantire, dunque, che le nuove tecnologie rappresentino un fattore di progresso, e non di regressione sociale, valorizzando anziché comprimendo le libertà affermate sul terreno lavoristico, è indispensabile garantirne la sostenibilità sotto il profilo democratico e la conformità ad alcuni irrinunciabili principi.

Lungi dal rappresentare un lusso da non potersi permettere in tempi difficili, la protezione dati ha dimostrato, da questo punto di vista, non solo di consentire tutto ciò che sia opportuno per il contrasto della pandemia, ma anche di poter fondare, attraverso le garanzie accordate ai nostri dati, quella fiducia

nel digitale senza la quale nessuna soluzione tecnica potrebbe mai avere successo.

Quale contributo utile all'attività di prevenzione sanitaria, abbiamo indicato, al Parlamento e al Governo, i principali criteri da seguire per migliorare l'efficacia delle misure adottate, in particolare rispetto al *contact tracing*, che sin da subito abbiamo richiesto tracciasse i contatti, non le persone.

Nel rilevare l'importanza dei principi di proporzionalità, necessità, adeguatezza cui devono conformarsi le scelte limitative dei diritti fondamentali, abbiamo indicato le diverse implicazioni delle varie soluzioni tecniche proposte, preferibili nella misura in cui riescano a minimizzare l'impatto sulla persona e la sua vita privata, pur garantendo l'attendibilità e l'efficacia dei risultati.

Analogo bilanciamento tra esigenze di sanità pubblica e tutela individuale abbiamo auspicato in relazione all'indagine di sieroprevalenza prevista rispetto al Covid 19, con indicazioni utili alla più efficace conduzione dello studio.

Rispetto alle varie circostanze sottoposteci abbiamo sottolineato la necessità di studiare modalità e ampiezza delle misure da adottare in vista della loro efficacia, gradualità e adeguatezza, senza preclusioni astratte o tantomeno ideologiche, ma anche senza improvvisazioni o velleitarie deleghe, alla sola tecnologia, di attività tanto necessarie quanto complesse.

3. La democrazia di fronte alla pandemia

Non è stato mai così evidente, come in questi mesi, che l'innovazione digitale abbia rappresentato un "fatto sociale totale", capace di inscrivere in nuove coordinate un'intera costruzione del mondo e la sua stessa antropologia. L'emergenza sanitaria ha evidenziato la necessità del ricorso alla tecnologia in funzione ausiliaria della scienza e la corrispettiva esigenza di valorizzare il digitale quale spazio immateriale in cui ritrovarsi.

E la protezione dati, regolando le condizioni per la circolazione di ciò che,

come il dato, rappresenta l'elemento costitutivo del digitale, in questo scenario si è rivelata un presupposto ineludibile di ogni possibile equilibrio tra l'uomo e la tecnica, la libertà e il determinismo algoritmico.

Le emergenze devono, del resto, poter contemplare anche alcune significative deroghe ai diritti, purché non irreversibili e proporzionate. Non devono essere, in altri termini, un punto di non ritorno ma un momento in cui modulare prudentemente il rapporto tra norma ed eccezione, coniugando istanza personalistica ed esigenze solidaristiche.

La duttilità del diritto, la sua capacità di adeguarsi al contesto riconoscendo gli adattamenti necessari e proporzionati alle specifiche esigenze, pur senza intaccare il "nucleo duro" dei diritti fondamentali, è la più grande forza della democrazia.

E questa forza sta dimostrando di avere il nostro Paese che, pur non nuovo a circostanze difficilissime, sta affrontando la prova più impegnativa dal secondo dopoguerra, utilizzando anche la tecnica in modo sostenibile, a fini di utilità sociale.

Il rischio che dobbiamo esorcizzare è quello dello scivolamento inconsapevole dal molto evocato modello coreano a quello cinese, scambiando la rinuncia a ogni libertà per efficienza e la biosorveglianza totalitaria per soluzione salvifica.

Così, una volta cessata questa difficile stagione, avremo forse imparato a rapportarci alla tecnologia in modo meno fideistico e più efficace, mettendola davvero al servizio dell'uomo.

Se c'è qualcosa che, forse, non tornerà più come prima, sarà il nostro rapporto con il digitale, di cui abbiamo compreso tutta l'ambivalenza e, dunque, la necessità di valorizzarne le straordinarie potenzialità "generative" contrastandone gli effetti nichilisti o anche solo regressivi.

Solo così sarà possibile fare tesoro della lezione di Tucidide, che ricordava come Atene fosse stata distrutta, più che dalla peste, dalla paura di questa.

4. Un circuito virtuoso

Ma anche in contesti diversi, nel corso di quest'anno, la protezione dei dati ha dimostrato di essere uno straordinario presupposto di democrazia, capace di coniugare personalismo e solidarismo, nascendo tra libertà e dignità, tra persona e società.

In linea generale, in questo secondo anno di applicazione della nuova disciplina, europea e di adeguamento interno, si è rivelata determinante l'interlocuzione con Parlamento e Governo, che in un circuito virtuoso ha consentito di migliorare, spesso sensibilmente, le norme proposte.

E' il caso, ad esempio, delle modifiche in tema di fascicolo sanitario elettronico, introdotte dal d.l. rilancio a seguito di un proficuo confronto con il Ministero della salute, o del reddito di cittadinanza, la cui disciplina attuativa ha concluso un percorso di collaborazione che ha contribuito a introdurre garanzie importanti per la riservatezza dei cittadini.

Rilevante si prospetta anche il confronto sul regolamento relativo agli obblighi di pubblicità inerenti i dirigenti pubblici, che dovrà conformarsi ai principi sanciti dalla sentenza 20/2019 della Corte costituzionale, in ordine al bilanciamento tra privacy e trasparenza dell'azione amministrativa.

Anche rispetto al registro pubblico delle opposizioni, il nostro parere sul regolamento attuativo della nuova disciplina ha rappresentato il punto di arrivo di un'interlocuzione - con le Camere prima e con il Governo poi - che ha consentito di rafforzare il contrasto del telemarketing selvaggio, sempre più invasivo e ramificato su plurimi rapporti commerciali.

Due tra le più elevate sanzioni irrogate quest'anno (una di oltre 27 e l'altra di oltre 11 milioni di euro) hanno, infatti, riguardato questo fenomeno, spesso indice sintomatico di una più generale negligenza rispetto agli obblighi sanciti in materia di protezione dati. Tale inosservanza è tanto più grave quanto più rilevante sia il patrimonio informativo societario che, in assenza di rigorose misure

di protezione dei dati, diviene vulnerabile terra di conquista per una sempre più abile criminalità informatica.

E' auspicabile che la consapevolezza del valore abilitante e pro-competitivo della protezione dei dati contribuisca a rendere questa disciplina parte essenziale del comune sentire.

Anche per questo è necessario completare, con gli ultimi tasselli, il quadro normativo interno emanando, in particolare, il regolamento attuativo del d.lgs. n. 51 del 2018, che dovrà definire le caratteristiche essenziali dei trattamenti svolti per fini di polizia e giustizia penale.

Un'ulteriore inerzia aggraverebbe la condizione di incertezza normativa che caratterizza aspetti, pur così rilevanti, della disciplina.

5. Equità fiscale e garanzie individuali

Le difficoltà proprie del contesto economico - già prima della pandemia - hanno reso urgente il recupero delle risorse sottratte dall'evasione: obiettivo essenziale per il nostro Paese, per garantire quell'equità fiscale "promessa" dalla Costituzione.

Per questo l'Autorità - pur assicurando il diritto dei cittadini al corretto trattamento dei loro dati - ha sempre supportato le misure volte a rafforzare l'efficacia dell'azione di contrasto dell'evasione fiscale, anche nell'ambito delle misure innovative introdotte in sessione di bilancio.

Lo sforzo con cui abbiamo tentato di promuovere un bilanciamento, il più equo possibile, tra l'efficacia delle verifiche fiscali e il diritto alla protezione dei dati personali è stato da alcuni scambiato per un ostacolo alle strategie adottate dall'amministrazione.

Quest'erronea rappresentazione - indifferente all'esigenza di mediazione propria di ogni scelta pubblica che riguardi una pluralità di interessi in gioco - stride con la lettera e lo spirito dei provvedimenti adottati dall'Autorità, in tale materia, durante l'intero mandato.

Ciascuno di essi, infatti, ha inteso garantire la sicurezza del patrimonio informativo dell'Agenzia delle entrate e l'esattezza dei dati (unitamente quindi all'affidabilità dei criteri di calcolo) sui quali si basano gli accertamenti, così migliorandone l'efficacia.

La profilazione sulla base del rischio fiscale - prevista sin dal 2011 - impone, infatti, l'adozione di garanzie volte a selezionare i dati effettivamente utili, escludendo quelli privi di rilievo e a correggere potenziali errori nel processo algoritmico conferendo così all'attività fiscale, anche nella percezione dei cittadini, quella più forte legittimazione che solo una combinazione equa di tecnologia e "fattore umano" può assicurare.

E' questo un profilo su cui abbiamo sollecitato l'attenzione del legislatore, anche relativamente al disegno di legge di bilancio.

Rispetto alla limitazione dei diritti dell'interessato prevista dalla stessa legge, abbiamo sottolineato la necessità di non escludere le possibilità di rettifica di dati inesatti, funzionale ad evitare valutazioni errate e quindi anche, in ipotesi, una falsa rappresentazione della capacità contributiva.

Tutt'altro che di ostacolo, dunque, l'azione del Garante si è rivelata semmai sinergica alla migliore efficacia degli accertamenti fiscali, nel rispetto peraltro del diritto dei cittadini a non essere erroneamente profilati come evasori.

La rappresentazione della protezione dati come ostacolo al libero dispiegamento dell'azione amministrativa (o delle indagini giudiziarie o della lotta all'evasione fiscale) è una costante del dibattito pubblico, che tuttavia mistifica in modo strumentale l'agire dell'Autorità.

6. Protezione dati e sovranità digitale

La contrapposizione, spesso insistita nel dibattito politico, tra protezione dati e interessi generali di varia natura rischia di oscurare, molto più spesso di quanto si creda, virtuose sinergie.

E' questo il caso della cybersecurity, il cui rapporto con la privacy è tutt'altro che antagonista, come abbiamo dimostrato con la proficua e consolidata collaborazione con il Copasir e con il Dis.

Questo, perché la sicurezza dello spazio cibernetico implica anzitutto, inevitabilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale con i suoi vari snodi.

E' la questione che abbiamo posto spesso in sede europea, da ultimo rispetto al social network Tik Tok, promuovendo accertamenti in ordine alle garanzie di sicurezza offerte, anche e soprattutto con riferimento ai dati degli utenti minorenni.

Su temi come questi, che toccano profondamente tanto la sicurezza collettiva quanto quella individuale, l'Europa deve infatti saper parlare con una voce sola, riflettendo quell'ambizione, insieme unificante e identitaria sottesa al Regolamento.

La fragilità strutturale e la scarsa consapevolezza dei potenziali bersagli di attività massive di *malware* acuisce, poi, la gravità degli attacchi, già rafforzata dal ricorso ad insidiose tecniche di intelligenza artificiale.

Gli attacchi sono ulteriormente cresciuti nello scorso anno: persino del 91,5% nel settore dei servizi on line e del cloud.

Gli atti di spionaggio/sabotaggio sono triplicati, in misura percentuale, rispetto allo scorso anno.

La pandemia ha ulteriormente acuito questo fenomeno rivoltosi, addirittura, ai danni di strutture sanitarie di eccellenza anche italiane, al punto che si è proposto di qualificare tali atti come propriamente terroristici.

Del resto, in un contesto in cui ciascun oggetto di uso quotidiano (si pensi agli assistenti vocali!) può rappresentare il canale d'ingresso di potenziali attacchi informatici, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture un obiettivo prioritario delle politiche pubbliche.

La crescente complessità dei sistemi genera, infatti, vulnerabilità sfruttate per paralizzare reti di servizi pubblici essenziali e canali di comunicazione di

primaria importanza, con un impatto, dunque, concretissimo sulla vita pubblica.

Sono ancora troppi e troppo importanti i sistemi informativi, soprattutto pubblici, caratterizzati da vulnerabilità suscettibili di pregiudicare tanto la sicurezza nazionale quanto la dignità dei soggetti i cui dati siano divulgati.

Il *data breach* dell'Inps, che ha determinato l'esfiltrazione di dati rivelatori anche di condizioni di fragilità economica è, in questo senso, significativo. Esso dimostra, peraltro, l'importanza della rigorosa osservanza delle regole di protezione dati, a fini tanto preventivi quanto remediali, se non altro per circoscrivere gli effetti delle violazioni, come è apparso evidente rispetto alle 1.443 notifiche di violazione dei dati personali ricevute dal Garante nel 2019, da parte di soggetti pubblici e privati.

Esse hanno riguardato tentativi di acquisizione di dati personali (credenziali di accesso, dati di contatto o relativi a strumenti di pagamento), accesso abusivo a mail e pec, perdita di dati per effetto di *ransomware* ecc..

Le implicazioni, in termini di sicurezza nazionale, di alcuni *data breach* dimostrano anche come la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" induca a ripensare il concetto di sovranità digitale.

E di fronte alla delocalizzazione in *cloud* di attività rilevantissime chiediamo al Parlamento e al Governo se non si debba investire in un'infrastruttura *cloud* pubblica, con stringenti requisiti di protezione, per riversarvi con adeguata sicurezza dati di tale importanza.

In un contesto in cui le tecnologie ICT sono divenute - sempre più chiaramente con la pandemia - la principale infrastruttura di ciascun Paese, assicurarne una regolazione sostenibile e adeguata, tale da garantire sicurezza, indipendenza dai poteri privati, soggezione alla giurisdizione interna, diviene un obiettivo non più eludibile.

7. Giustizia, tecnologia, dignità

Le esigenze di giustizia e la privacy dei cittadini sono i fuochi dell'ellisse su cui si sviluppa una dinamica essenziale per la democrazia, resa inevitabilmente più complessa dalle potenzialità delle nuove tecnologie.

Uno dei campi in cui questa tensione si manifesta con maggiore urgenza è quello delle intercettazioni, rispetto alla quale, sin dalla prima fase dell'esame della riforma "Orlando", abbiamo sollecitato l'esigenza di una più puntuale selezione del materiale investigativo assicurando, nel rispetto dei diritti della difesa, che negli atti processuali non siano riportati interi spaccati di vita privata estranei al tema di prova, bilanciando privacy ed esigenze di giustizia.

Le misure, previste dalla riforma del 2017, volte a limitare la circolazione endoprocessuale delle intercettazioni eccedenti le esigenze investigative hanno segnato un'importante innovazione, che - come abbiamo rappresentato in Parlamento - è bene conservare, anche con la nuova disciplina, almeno come obbiettivo, pur modulando diversamente gli oneri di polizia giudiziaria e pubblico ministero in questa fase.

La derubricazione del divieto di trascrizione in dovere di vigilanza dell'organo requirente gli impone dunque, per non vanificare la portata innovativa della riforma, un vaglio attento sull'effettivo rispetto di questo canone di minimizzazione.

Per quanto invece concerne le intercettazioni mediante captatori, sarebbe stato opportuno cogliere l'occasione del decreto-legge per colmare le lacune normative già da noi rilevate rispetto alla riforma Orlando e ribadite con la segnalazione sul caso Exodus.

Le straordinarie potenzialità intrusive di tali strumenti impongono - come è emerso per altri versi nelle scorse settimane - garanzie adeguate per impedire che essi, da preziosi ausilii degli inquirenti, degenerino in mezzi di sorveglianza massiva o, per converso, in fattori di moltiplicazione esponenziale delle vulnerabilità del compendio probatorio, rendendolo estremamente permeabile se allo-

cato in server non sicuri o, peggio, delocalizzati anche al di fuori dei confini nazionali.

Più in generale, abbiamo auspicato un supplemento di riflessione in ordine alla progressiva estensione dell'ambito applicativo del *trojan*, che dovrebbe invece restare circoscritto.

E' significativo che la Corte costituzionale tedesca abbia censurato la disciplina di tale tipo d'intercettazioni (sia pure preventive), per violazione non solo della riserva di giurisdizione ma anche del principio di proporzionalità.

Va infatti sottolineata l'intrinseca diversità, rispetto alle intercettazioni tradizionali, di quelle mediante captatori, propria della loro capacità invasiva e dell'attitudine a esercitare una sorveglianza ubiquitaria, con il rischio peraltro di rendere più difficile il controllo ex post sulle operazioni compiute sul dispositivo-ospite. Di qui l'esigenza di un rigoroso rispetto del principio di proporzionalità, a tutela del "generale diritto alla libertà del cittadino nei confronti dello Stato".

Questo dev'essere il parametro essenziale da osservare nella disciplina di strumenti investigativi che devono poter garantire tanto la sicurezza quanto la libertà, secondo la sinergia che richiedono la normativa costituzionale e sovranazionale.

In questo senso, è indifferibile una revisione organica della disciplina della conservazione dei dati di traffico, i cui termini - sei anni - appaiono difficilmente compatibili con la necessaria proporzionalità delle limitazioni della privacy rispetto alle esigenze investigative, posta dalla Corte di giustizia a fondamento della declaratoria di illegittimità della direttiva 2006/24/CE (basata su un termine massimo di due anni).

8. Il pendio scivoloso

Analoga proporzionalità deve caratterizzare il ricorso alle straordinarie potenzialità dell'intelligenza artificiale, tra le quali quelle connesse al riconosci-

mento facciale, che può essere o meno compatibile con i diritti fondamentali in ragione dei limiti cui soggiaccia, commisurati appunto ai rischi implicati.

A tali fini, è determinante la cognizione reale delle implicazioni di ordine individuale, sociale, persino etico della tecnologia considerata.

Per questo, avevamo guardato con favore alla proposta europea di moratoria sul riconoscimento facciale, ritenendola una lungimirante affermazione dei principi di precauzione e prevenzione, anche considerando la varietà di usi ai quali tale tecnica può prestarsi.

Se infatti, in alcuni ambiti il ricorso a tali sistemi, circoscritto e assistito da garanzie adeguate, può fornire un contributo difficilmente conseguibile altrimenti, in altri contesti esso può invece risolversi in un'ingiustificata (perché, appunto, sproporzionata) limitazione dei diritti individuali.

Il ricorso diffuso a queste tecniche in circostanze "ordinarie" e a meri fini agevolatori, rischia peraltro di indurre a sottovalutarne l'invasività: il pericolo è quello del "pendio scivoloso", fino all'acritica accettazione sociale della progressiva perdita di libertà.

E questo, tanto più in ragione dei limiti che il consenso incontra rispetto alla biometria cosiddetta facilitativa, di cui spesso si ignorano le implicazioni: dalla ubiquitaria geolocalizzazione alla sempre più penetrante profilazione.

Il tutto, in un contesto di generale asimmetria informativa tra soggetto passivo e attivo della raccolta dei dati, in cui le tradizionali diseguaglianze rischiano di ripresentarsi in forma tanto più incisiva quanto più sottile.

Sarà dunque determinante, in questo senso, il rispetto dei principi di necessità e proporzionalità nel ricorso a tali misure: criteri essenziali su cui le Corti europee hanno sinora fondato un rapporto armonico tra libertà, tecnologia e sicurezza.

E saranno importanti le scelte regolatorie che dovessero, eventualmente, legittimare l'uso del riconoscimento facciale a fini di polizia. La previsione normativa consente infatti di stabilire garanzie e limiti uniformi su tutto il territorio nazionale, come abbiamo avuto modo di sottolineare rispetto ad alcune iniziative

di enti locali, secondo uno schema destinato a riproporsi in assenza di una cornice regolatoria unitaria.

9. Il più universale dei diritti

Uno degli ambiti in cui il diritto alla protezione dati ha dimostrato di svolgere un essenziale ruolo arbitrale tra diritti fondamentali è quello dell'amplificazione dei contenuti informativi determinata dalla rete.

La giurisprudenza interna, quella della Corte di giustizia e la nostra prassi hanno contribuito a regolare un contesto, quale in particolare quello del diritto all'oblio, in cui più evidenti appaiono le vicendevoli implicazioni tra tecnica e diritto: come la prima muti lessico e semantica del secondo e come questo imponga, alla prima, soluzioni inedite a nuove tensioni.

Che, in quest'ambito, riguardano il mutamento del rapporto tra storia e biografia, giudizio pubblico e soggettività, determinato dalla capacità della rete di attribuire a ciascuno nuove identità, spesso insensibili al trascorre del tempo, ma tali da recare grave pregiudizio all'interessato. Lo dimostra il numero di istanze rivolteci anche quest'anno, che rappresentano una quota significativa delle 8.092 cui abbiamo fornito riscontro. Anche per questo abbiamo ritenuto, in alcuni casi, di accordare tutela rispetto ai profili stilati utilizzando chiavi di ricerca integrative o diverse rispetto al nome se idonee a meglio identificare, sia pur indirettamente, l'interessato.

Il profilo della persona, stilato dal motore di ricerca organizzando le notizie indicizzate - come ha sottolineato anche la Corte di giustizia - deve del resto rifletterne la condizione (anche giudiziaria) attuale.

La notizia dell'assoluzione non deve, ad esempio, essere posta in coda a una pluralità di link più risalenti, relativi all'imputazione, alle misure cautelari, persino alla condanna non definitiva.

Dev'essere, insomma, il criterio dell'esattezza e dell'aggiornamento - e non

quello del numero dei *click* - a governare l'algoritmo dei motori di ricerca i quali, titolari di un ruolo sempre più centrale rispetto all'informazione in rete, non possono affidare al solo procedimento informatico decisioni così rilevanti sui diritti fondamentali.

Significativo, in tal senso, il nostro orientamento con cui abbiamo ritenuto meritevole di deindicizzazione notizie di condanne non aggiornate al percorso, spesso complesso, successivamente compiuto dal soggetto, nel frattempo riabilitato.

La nostra prassi, così come la giurisprudenza europea e interna, mira così a responsabilizzare ulteriormente le piattaforme rispetto ad attività che hanno un impatto determinante sui diritti fondamentali, utilizzando anche la tecnica come soluzione di molte contraddizioni da essa stessa ingenerate.

E questa funzione "libertaria" della tecnica sembra, del resto, promossa da un'ulteriore sentenza della Corte di giustizia che, poche settimane dopo la pronuncia appena descritta, ha ammesso che i giudici possano - con "un'ingiunzione dinamica" - ordinare la rimozione di contenuti equivalenti a quelli già dichiarati illeciti, con effetto esteso anche a livello globale.

Tutelare la dignità limitatamente a una porzione di contenuti visibili solo su scala nazionale, infatti, sarebbe meramente velleitario in un contesto, quale quello della rete, che ha superato l'idea della frontiera.

La Corte sembra consapevole di come il diritto alla protezione dati - il più transnazionale dei diritti, in quanto si esercita su di uno spazio, quale quello digitale, che non conosce confini - necessiti di una tutela altrettanto sovranazionale ed aspiri a un riconoscimento universalistico che sembra ormai sempre più urgente.

Anche con la sentenza Google-Cnil, pur negando la sussistenza di un obbligo di deindicizzazione globale secondo la disciplina di protezione dati, la Corte ha infatti ammesso la possibilità di accordare, in ragione delle peculiarità del caso concreto, anche tale forma di tutela espansiva.

10. Tecnologie "ribelli"

In assenza di garanzie realmente uniformi a livello globale, infatti, la rete continuerà a riproporre al suo interno enclave anomiche in cui possano agire indisturbati quanti intendano sfruttare le straordinarie potenzialità del digitale per violare diritti, anziché promuoverli.

E' il problema che, ad esempio, rispetto alle fake news abbiamo discusso in sede di audizione alla Camera e su cui abbiamo istituito un tavolo di lavoro con l'Agcom.

Ma è un profilo che - ricondotto al tema più generale dell'uso distorsivo e spesso anche ritorsivo della rete (si pensi al *revenge porn*) - sollecita una riflessione avulsa da pregiudizi.

La tendenziale eliminazione, nel mondo della rete, della distinzione tra produttori e destinatari dell'informazione ha avuto, da un lato, lo straordinario pregio di espandere le possibilità di libera manifestazione del pensiero e di accesso all'informazione, da parte anche delle fasce più marginali della popolazione.

Dall'altro lato, tuttavia, ha amplificato la diffusione di notizie false e spesso diffamatorie, per la maggiore capacità aggregativa che hanno - nell'età della rabbia e della disintermediazione - i contenuti offensivi, capaci di polarizzare consensi nella lotta all'altro-da-sé.

L'autismo informativo e l'effetto "ecocamera digitale" finiscono così per produrre non già informazione ma "auto-comunicazione di massa", anche grazie alla non neutralità dell'indicizzazione e della gerarchia algoritmica. Nel conferire maggiore o minore visibilità ai contenuti, infatti, queste tecniche incidono in maniera significativa sul diritto d'informazione, con il rischio di una censura privata o comunque di una selezione informativa che non risponda più a valori socialmente condivisi, ma a un'insindacabile legge del mercato.

Le piattaforme sono oligopoliste non tanto e non solo perché detengono un potere economico rilevantissimo, quanto perché dispongono della principale

infrastruttura sociale: prima ancora di conquistare il mercato, orientano il pensiero sfruttando la potenza dei dati.

Di qui la pluralità di funzioni della protezione dati che, governando le condizioni per il legittimo uso dei dati personali, rafforza le tutele consumeristiche, regola l'esercizio del potere informativo e tutela intangibili spazi di autodeterminazione individuale, rispetto al *"nudging"* praticato a fini commerciali, ideologici, persino politici.

E quanto più si fa spazio sociale e politico, tanto più la rete deve poter garantire le sue caratteristiche di democraticità, universalità, apertura e libertà nell'accesso, che ne hanno consentito l'affermazione come il più grande spazio pubblico conosciuto dall'umanità.

La rilevanza dei poteri privati è, in tale contesto, un tema da affrontare assieme a quello della regolazione del digitale, favorendo sì la responsabilizzazione dei gestori, ma riservando la decisione sui diritti fondamentali, in ultima istanza, all'autorità pubblica, secondo il modello che la protezione dati ha offerto sul terreno dell'oblio o del cyberbullismo.

Si dovrebbe allora, forse, riflettere sulla regolazione dell'uso dell'anonimato, rendendolo realmente reversibile. Ma, pur al netto delle criticità da cui non sarebbe scevra alcuna soluzione in tal senso, anch'essa sarebbe del tutto velleitaria in assenza di uniformità, sul piano internazionale, di una tale disciplina, che, bilanciando libertà di espressione e dignità, dovrebbe rendere effettiva la tutela delle vittime di illeciti on-line.

Quell'unificazione normativa che l'Europa ha voluto promuovere - non senza un investimento identitario importante - sulla protezione dati, quale necessario presupposto di ogni regolazione possibile del digitale, dovrebbe essere quindi, oggi, un obiettivo condiviso della comunità internazionale.

E parallelamente alla cogenza e alla forza, anche simbolica, della norma, dovrebbe promuoversi una tecnologia 'ribelle' alle prevaricazioni e alle discriminazioni (per dirla con Morozov), con funzione cioè ausiliaria del progresso sociale.

In questo senso, andrebbe percorsa la strada di soluzioni tecniche volte a segnalare all'utente, in base a criteri oggettivi contenuti potenzialmente inaffidabili stimolando anche, così, il senso critico del pubblico.

Utilizzare la tecnica in funzione di promozione, anziché di limitazione, dei diritti può essere, in questo senso, una delle soluzioni migliori per contribuire a rendere la rete quello straordinario strumento pluralista che doveva e deve essere, promuovendone la sostenibilità.

11. Cronaca, storia, orizzonti

Questa è la direzione rispetto alla quale la protezione dati ha dimostrato di poter fornire un contributo essenziale, per una declinazione in chiave democratica del digitale, secondo l'auspicio già espresso da Stefano Rodotà e Giovanni Buttarelli, la cui mancanza sempre avvertiamo.

Perseguire quest'obbiettivo contribuirà a consolidare quel particolare profilo identitario che l'Europa sta progressivamente affermando sul terreno del rapporto tra diritto e tecnica, tentando di rimodularlo in chiave antropocentrica, perché il "destino dell'Occidente" non contraddica, con la cronaca, la propria storia.

E in quest'affermazione identitaria di "umanesimo digitale", la protezione dati assume una sempre più insostituibile funzione di salvaguardia dello Stato di diritto, di fronte alle continue tensioni imposte dalla sinergia di tecnica, potere e persino emergenza, essendo strumento di governo non solo dell'identità individuale, ma anche dell'umanità rispetto alla potenza di calcolo.

Questa disciplina, con la sua vocazione unitaria, ha così rappresentato il più organico tentativo di regolazione delle nuove tecnologie: una vera e propria Costituzione per il digitale, che un numero sempre crescente di ordinamenti ha assunto a modello.

Ma la sfida sarà vinta solo se e quando la protezione dei dati diverrà, fino in

fondo, cultura e sentire diffuso di tutti. Che, come tale, deve essere affidata non alla deterrenza o alla repressione sanzionatoria ma alla consapevolezza di come la sostenibilità del futuro dipenda, in larga parte, dalla tutela che sapremo accordare ai frammenti del nostro io e del nostro vissuto.

Questo è l'orizzonte che, con il Collegio che ho avuto l'onore di presiedere, riteniamo di indicare a chi avrà la responsabilità e il privilegio di guidare un'Autorità, come questa, sempre più centrale per la vita democratica del Paese e sempre più vicina alle persone.

Signor Presidente, la nostra attività è stata prorogata oltre ogni ragionevole misura.

L'invito che, con rispetto, attraverso la Sua persona, rivolgo al Parlamento è quello di procedere quanto prima all'elezione dei nuovi componenti.

Per concludere, consentitemi di rivolgere un sincero ringraziamento al Segretario generale e a tutti coloro che, nell'Ufficio, ogni giorno si impegnano con generosità e competenza per rispondere alla crescente domanda di tutela dei cittadini.

E ringrazio, ancora una volta, le Colleghe Augusta Iannini, Giovanna Bianchi Clerici, Licia Califano, componenti il Collegio del Garante: insieme abbiamo condiviso un lungo mandato e una preziosa amicizia.

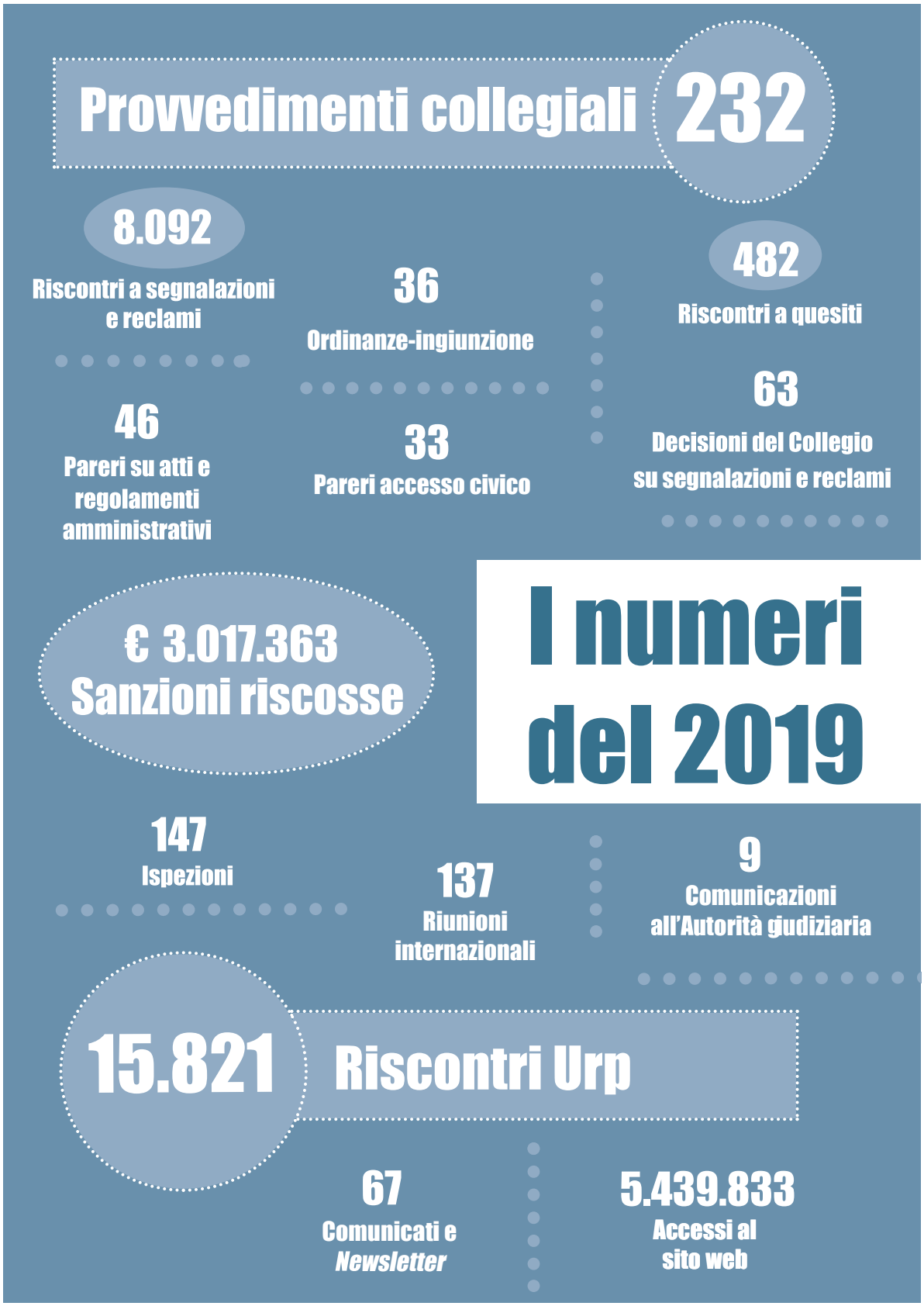
GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Relazione2019

www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza Venezia, 11
00187 Roma
tel. 06 696771
email: protocollo@gpdp.it
www.garanteprivacy.it


Provvedimenti collegiali 232
8.092
Riscontri a segnalazioni e reclami
36
Ordinanze-ingiunzione
482
Riscontri a quesiti
46
Pareri su atti e regolamenti amministrativi
33
Pareri accesso civico
63
Decisioni del Collegio su segnalazioni e reclami
I numeri del 2019
€ 3.017.363
Sanzioni riscosse
147
Ispezioni
137
Riunioni internazionali
9
Comunicazioni all'Autorità giudiziaria
15.821
Riscontri Urp
67
Comunicati e Newsletter
5.439.833
Accessi al sito web

PAGINA BIANCA

Indice

Indice

I - STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Introduzione 3

2. Il quadro normativo in materia di protezione dei dati personali 14

2.1. Le modifiche al Codice 14
2.2. Le leggi di particolare interesse per la protezione dei dati personali 15
2.3. Norme di rango secondario 33

3. I rapporti con il Parlamento e le altre Istituzioni 34

3.1. L'attività consultiva del Garante 34
3.1.1. La consultazione del Garante su atti normativi statali di rango primario: le audizioni in Parlamento su progetti di legge 34
3.1.2. La consultazione del Garante su atti normativi statali di rango primario: i pareri su schemi di decreto legislativo 35
3.1.3. La consultazione del Garante su atti normativi delle regioni e delle autonomie 37
3.1.4. I pareri sugli atti regolamentari e amministrativi del Governo 37
3.1.5. I pareri sugli atti regolamentari e amministrativi resi ad altre Istituzioni 39
3.2. Le attività di sindacato ispettivo e di indirizzo e controllo del Parlamento 41
3.3. L'esame delle leggi regionali al vaglio di costituzionalità del Governo 41

II - L'ATTIVITÀ SVOLTA DAL GARANTE

4. Il Garante e le amministrazioni pubbliche 47

4.1. L'attività fiscale e tributaria 47
4.1.1. La cd. dichiarazione dei redditi precompilata 47
4.1.2. Controlli antievasione: l'utilizzo dell'Archivio dei rapporti finanziari 48
4.1.3. L'utilizzo di dati derivanti dallo scambio automatico obbligatorio tra autorità fiscali estere aderenti agli accordi internazionali 49
4.1.4. Analisi del rischio per la lotta all'evasione fiscale: la legge di bilancio 2020 49
4.1.5. La lotteria dei corrispettivi 52
4.1.6. Le biglietterie automatizzate 53
4.1.7. La fatturazione elettronica 54
4.2. La previdenza e l'assistenza sociale 57
4.2.1. Il reddito e la pensione di cittadinanza 57
4.2.2. L'Isee precompilato 60
4.3. Vigilanza su altre grandi banche dati pubbliche 62
4.4. L'istruzione 65
4.5. La trasparenza amministrativa e la pubblicità dell'azione amministrativa 67
4.5.1. La pubblicazione di dati personali online 67
4.5.2. L'accesso civico 68

Indice

4.5.3. L'accesso ai documenti amministrativi 75
4.6. I trattamenti effettuati presso regioni ed enti locali 75
4.7. La materia anagrafica ed elettorale 76
4.8. I trasferimenti di dati personali verso autorità pubbliche o organizzazioni internazionali 78
4.9. L'attività svolta in relazione ai Responsabili della protezione dei dati in ambito pubblico 80

5. La sanità e la ricerca 82
5.1. I trattamenti di dati per fini di cura 82
5.1.1. Il trattamento dei dati personali riferiti ai pazienti per finalità ulteriori rispetto alla cura 84
5.2. Il Fascicolo sanitario elettronico e il *dossier* sanitario 85
5.3. I trattamenti di dati relativi alle condizioni di salute per fini amministrativi 87
5.4. I chiarimenti rispetto alle innovazioni normative in ambito sanitario 89
5.4.1. L'esercizio dei diritti in ambito sanitario 91
5.4.2. La valutazione d'impatto in ambito sanitario 91
5.4.3. I chiarimenti in relazione ai Responsabili della protezione dei dati e le attività con le reti dei Rpd del settore della sanità e della ricerca 92
5.5. La ricerca 93
5.5.1. Prescrizioni relative al trattamento dei dati genetici e al trattamento dei dati personali effettuato per scopi di ricerca scientifica 93
5.5.2. Parere in ordine al trattamento dei dati personali, anche inerenti a particolari categorie di dati, per finalità di ricerca medica, biomedica e epidemiologica 96

6. La statistica 97
6.1. Parere sull'indagine europea sulla salute (*European Health Interview Survey* - EHIS IST-02565) 97

7. I trattamenti in ambito giudiziario e da parte di Forze di polizia 100
7.1. I trattamenti in ambito giudiziario 100
7.2. I trattamenti da parte di Forze di polizia 103
7.3. Il controllo sul sistema di informazione Schengen 103

8. L'attività giornalistica 105
8.1. Premessa 105
8.2. Dati statistici ed aspetti procedurali 105
8.3. Il trattamento dei dati nell'esercizio dell'attività giornalistica 107
8.3.1. Dati giudiziari 107
8.3.2. Dati relativi a minori 109
8.3.3. Registrazioni audio e video 109
8.4. Diffusione di dati personali sui *social network* 109
8.5. Trattamento dei dati tramite i motori di ricerca 110

Indice

9. Cyberbullismo 116

10. *Marketing* e trattamento dei dati personali 118

10.1. *Telemarketing* 118

11. Internet e servizi di comunicazione elettronica 122

11.1. Trattamenti di dati nel settore telefonico 122

11.2. Raccolta dei dati *online* per finalità di *marketing* e profilazione 123

11.3. Attività svolta in relazione ai trattamenti di dati personali a fini di propaganda elettorale 125

11.4. Procedure IMI relative a trattamenti di dati in internet e in materia di comunicazioni elettroniche 127

12. Il trattamento dei dati personali da parte di movimenti politici e associazioni 131

13. La protezione dei dati personali nel rapporto di lavoro privato e pubblico 133

13.1. La protezione dei dati nell'ambito del rapporto di lavoro privato tra vecchia e nuova disciplina 133

13.2. Il trattamento di categorie particolari di dati nell'ambito del rapporto di lavoro: dall'autorizzazione generale al provvedimento prescrittivo del Garante ex art. 21, d.lgs. n. 101/2018 134

13.3. Controlli sulla posta elettronica aziendale successivamente alla cessazione del rapporto di lavoro 136

13.4. Il trattamento di dati dei dipendenti effettuato mediante dispositivi tecnologici indossabili 137

13.5. Il trattamento di dati contenuti in una relazione investigativa relativi ad un terzo 138

13.6. Compiti e responsabilità dei professionisti che effettuano trattamenti di dati personali su incarico del datore di lavoro 138

13.7. La limitazione dell'esercizio dei diritti dopo le modifiche al Codice 140

13.8. Il trattamento di dati di dipendenti pubblici e di utenti mediante il sistema di prenotazione e gestione dei servizi 141

13.9. Comunicazione di dati dei dipendenti a un ordine professionale 142

13.10. Inconfigurabilità del silenzio-assenso nel procedimento di autorizzazione amministrativa all'installazione ed utilizzo di impianti audiovisivi dai quali possa derivare la possibilità di controllo a distanza dei lavoratori 143

13.11. I trattamenti di dati nell'ambito dell'acquisizione e gestione delle segnalazioni in materia di *whistleblowing* 143

13.12. Il trattamento di dati biometrici dei dipendenti pubblici per finalità di rilevazione delle presenze 144

13.13. Il trattamento di dati nell'ambito di procedimenti disciplinari e delle procedure di protocollazione degli atti 145

13.14. I trattamenti di dati da parte del medico competente 147

Indice

14. Le attività economiche 149

14.1. Configurazione dei ruoli *privacy* nelle gare per l'affidamento dei servizi assicurativi 149

14.2. Il trattamento dei dati in ambito bancario e assicurativo 149

14.2.1. Data breach *nel settore bancario* 152

14.3. Dai codici di deontologia nel settore economico e finanziario ai codici di condotta 152

14.3.1. Il codice di condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale 153

14.3.2. Il codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti 153

14.4. La videosorveglianza in ambito privato 154

14.5. Trattamenti di dati in ambiti e settori particolari 154

14.5.1. Riconoscimento facciale dei passeggeri presso gli aeroporti di Roma Fiumicino e Milano Linate 154

14.5.2. Fornitura di energia elettrica e gas e trattamento di dati personali della clientela 155

14.5.3. Propaganda elettorale 156

14.6. Procedure IMI relative a trattamenti di dati in ambito economico 157

14.7. Accreditamento e certificazioni 158

15. Il trattamento dei dati personali nell'ambito del condominio 160

16. Violazione dei dati personali 161

17. Il trasferimento dei dati personali all'estero 162

18. L'attività ispettiva 163

18.1. I poteri di indagine e il nuovo regolamento del Garante n. 1/2019 163

18.2. La collaborazione con la Guardia di finanza 163

18.3. La programmazione dell'attività ispettiva 164

18.4. I principali settori oggetto di controllo 165

18.5. I provvedimenti adottati dal Garante a seguito dell'attività ispettiva 166

19. L'attività sanzionatoria 167

19.1. Violazioni penali 167

19.2. Sanzioni amministrative adottate in relazione alla disciplina previgente 167

19.3. Riscossione coattiva delle sanzioni 170

19.4. Versamenti relativi alle sanzioni amministrative 171

19.5. Il quadro sanzionatorio introdotto dal RGPD 171

20. Il contenzioso giurisdizionale 173

20.1. Considerazioni generali 173

20.2. I profili procedurali 173

Indice

20.3. Le opposizioni ai provvedimenti del Garante 173
20.4. L'intervento del Garante nei giudizi relativi all'applicazione del Codice 181

21. Le relazioni comunitarie e internazionali 182
21.1. La cooperazione tra le autorità di protezione dati nello Spazio economico europeo: il Comitato europeo per la protezione dei dati 182
21.2. La cooperazione delle autorità di protezione dei dati nel settore libertà, giustizia e affari interni 202
21.3. La partecipazione dell'Autorità in seno al Consiglio d'Europa e ad altri gruppi di lavoro internazionali 204
21.4. Le Conferenze internazionali ed europee 211
21.5. I progetti per l'applicazione del RGPD finanziati dall'UE: T4DATA e SMEDATA 213

22. Attività di normazione tecnica internazionale e nazionale 216

23. L'attività di comunicazione, informazione e di rapporto con il pubblico 217
23.1. La comunicazione del Garante: profili generali 217
23.2. I prodotti informativi 219
23.3. Il sito istituzionale, i prodotti multimediali e le pubblicazioni 220
23.4. Le manifestazioni e le conferenze 221
23.5. L'assistenza al pubblico e la predisposizione di nuovi strumenti informativi 224

24. Studi e documentazione 227

III – L'UFFICIO DEL GARANTE

25. La gestione amministrativa e dei sistemi informatici 231
25.1. Il bilancio e la gestione economico-finanziaria 231
25.2. L'attività contrattuale, la logistica e la manutenzione dell'immobile 233
25.3. L'organizzazione dell'Ufficio 234
25.4. "Autorità trasparente" e adempimenti relativi alla disciplina anticorruzione 238
25.5. Il settore informatico e tecnologico 240

IV – I DATI STATISTICI

Avvertenza ed elenco delle abbreviazioni e degli acronimi più ricorrenti

La presente Relazione è riferita al 2019 e contiene talune notizie già anticipate nella precedente edizione nonché informazioni relative agli sviluppi più recenti che si è ritenuto opportuno menzionare.

Arera	Autorità di regolazione per energia reti e ambiente
Agcom	Autorità per le garanzie nelle comunicazioni
AgID	Agenzia per l'Italia Digitale
all.	allegato
Anac	Autorità nazionale anticorruzione
art.	articolo
Bcr	*Binding corporate rules*
c.c.	codice civile
C.d.S.	Consiglio di Stato
c.p.	codice penale
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
Cad	codice dell'amministrazione digitale
cap.	capitolo
CDFUE	Carta dei diritti fondamentali dell'Unione europea
cd.	cosiddetto/i
CEDU	Carta europea dei diritti dell'uomo
cfr.	confronta
CGUE	Corte di giustizia dell'Unione europea
cit.	citato
Codice	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101)
Cepd	Comitato europeo per la protezione dei dati
cons.	considerando
Consob	Commissione nazionale per le società e la borsa
Corte EDU	Corte europea dei diritti dell'uomo
Cost.	Costituzione
d.d.l.	disegno di legge
d.l.	decreto-legge
d.lgs.	decreto legislativo
d.m.	decreto ministeriale

d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
doc.	documento
es.	esempio
Fse	Fascicolo sanitario elettronico
Gepd	Garante europeo per la protezione dei dati
G.U.	Gazzetta ufficiale della Repubblica italiana
GUUE	Gazzetta ufficiale dell'Unione europea
Gruppo Art. 29	Gruppo dei garanti europei istituto dall'art. 29 della direttiva 95/46/CE
IMI	*Internal Market Information System*
Ivass	Istituto per la vigilanza sulle assicurazioni
IWGDPT	*International Working Group on Data Protection in Telecommunications*
l.	legge
lett.	lettera
Mef	Ministero dell'economia e delle finanze
Mise	Ministero dello sviluppo economico
Miur	Ministero dell'istruzione dell'università e della ricerca
n.	numero
p.	pagina
p.a.	pubblica amministrazione
par.	paragrafo
Pec	posta elettronica certificata
provv.	provvedimento del Garante
r.d.	regio decreto
reg.	regolamento
RGPD	Regolamento (UE) 679/2016
Rdc	Reddito di cittadinanza
Rpd	Responsabile della protezione dei dati
Rpo	Registro pubblico delle opposizioni
sez.	sezione
Spid	Sistema pubblico dell'identità digitale
Ssn	Servizio sanitario nazionale
tab.	tabella
t.u.	testo unico
TFUE	Trattato sul funzionamento dell'Unione europea
Tulps	Testo unico delle leggi di pubblica sicurezza
UE	Unione europea
URL	*Uniform Resource Locator*
v.	vedi

PAGINA BIANCA