Quaderni del Dipartimento di Giurisprudenza
dell'Università di Torino

L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale

A cura di Roberto Cavallo Perin

Con il coordinamento editoriale di Isabella Alberti

UNIVERSITÀ DEGLI STUDI DI TORINO

QUADERNI DEL DIPARTIMENTO DI GIURISPRUDENZA
DELL'UNIVERSITÀ DI TORINO
20/2021

L'amministrazione pubblica con i *big data*: da Torino un dibattito sull'intelligenza artificiale

a cura di
Roberto Cavallo Perin

con il coordinamento editoriale di Isabella Alberti

UNIVERSITÀ DEGLI STUDI DI TORINO

Opera finanziata con il contributo del Dipartimento di Giurisprudenza dell'Università di Torino

La presente opera è stata sottoposta a revisione da parte di una Commissione di Lettura di docenti del Dipartimento nominata dal Comitato Scientifico della Collana in conformità al Regolamento delle pubblicazioni del Dipartimento di Giurisprudenza dell'Università di Torino.

Quaderni del Dipartimento di Giurisprudenza dell'Università di Torino

L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale, a cura di Roberto Cavallo Perin

Via Verdi, 8 – 10124 Torino
www.collane.unito.it/oa/
openaccess@unito.it

ISBN: 9788875901806

Prima edizione: marzo 2021

Grafica, composizione e stampa: Rubbettino Editore

Indice

Lunedì 20 maggio - I sessione
Algoritmi e diritto

Martedì 21 maggio - II sessione
Big data e attività conoscitiva della pubblica amministrazione

Martedì 21 maggio - III sessione
Interoperabilità delle banche dati e funzione amministrativa

Benedetto Ponti

L'amministrazione come fornitore e come fruitore di dati personali pubblici: sono praticabili soluzioni basate sulla *Big Data Analytics*/*Machine Learning*?

Abstract: L'articolo affronta il tema del regime giuridico dei dati pubblici, alla luce delle regole poste dal Regolamento generale per la protezione dei dati personali alla pubblica amministrazione: il principio di finalità cristallizzato dal Regolamento si traduce per l'amministrazione pubblica in un rafforzamento del principio di legalità a cui la stessa deve sottostare. L'articolo evidenzia che dalla convergenza di questi principi deriva un regime di gestione dei dati pubblici più rigoroso e stringente rispetto alla gestione privata, tale da rappresentare un potenziale ostacolo alla sperimentazione del machine learning nel settore pubblico. In particolare, lo specifico regime di gestione dei dati pubblici incide sulle modalità in cui i dati devono essere resi disponibili verso i terzi e quindi sugli obblighi che la pubblica amministrazione ha in quanto "fornitore" di dati e nondimeno sulle modalità di raccolta degli stessi poiché l'amministrazione -in quanto "fruitrice" di dati- deve procedere alla raccolta in un modo funzionalizzato all'interesse pubblico.

1. *Prima premessa: il framework asimmetrico*

L'amministrazione raccoglie, conserva e gestisce una mole enorme di dati personali, le cui potenzialità sono ben lungi dall'essere pienamente sfruttate secondo le logiche e le tecniche di elaborazione della *Big Data* analytics (BDA) e del Machine Learning (ML), per la significativa, fondante ragione che l'uso di questi dati raccolti e detenuti dal settore pubblico è soggetto ad un regime che – a tutela della libertà, della dignità, della riservatezza, etc. – ne regola in modo stringente l'utilizzo.

Tale regime – si intende, quello relativo all'uso dei dati personali da parte del settore pubblico – ha specifiche caratteristiche che, sotto l'apparente omogeneità delle regole poste a tutela dei dati personali così come disegnate dal GDPR[1], vedono nettamente distinti i presupposti di raccolta e di utilizzo dei dati personali da parte dei soggetti che esercitano funzioni un potere o una funzione pubblica, rispetto a tutti gli altri soggetti dell'or-

1. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 - Regolamento generale sulla protezione dei dati.

dinamento. Infatti, mentre questi ultimi hanno come fine il perseguimento di un "legittimo interesse" autonomamente individuato[2] e come presupposto di liceità all'uso innanzitutto il consenso dell'interessato, nel caso dei titolari (del trattamento) che esercitano un potere o una funzione pubblica il fine è integralmente etero-determinato[3], mentre la raccolta e l'uso dei dati generalmente (salvo alcune categorie di dati particolari) prescinde dal consenso dell'interessato. La raccolta e l'uso risultano in questo caso leciti solo nella misura in cui il loro trattamento sia connesso al perseguimento della finalità/compito di interesse pubblico così come definito dal legislatore ed affidato o "attribuito" all'amministrazione (o al privato che eserciti una funzione pubblica conferita dalla legge).

Il principio di finalità, connesso al presupposto di raccolta e utilizzo dei dati personali, proietta in modo forte il principio di legalità sul trattamento dei dati personali da parte della pubblica amministrazione, alla quale risulta precluso l'uso di dati personali al di fuori del perimetro di liceità disegnato dalla interazione tra principio di legalità (attribuzione di un potere/di un compito di interesse pubblico da parte della legge) e principio di finalità (che è proprio del regime del GDPR).

In verità, il principio di finalità si proietta ben oltre il perimetro dell'esercizio delle funzioni pubbliche, costituendo in effetti una sorta di *grundnorm* che permea ed informa di sé tutta la disciplina eurounitaria di tutela/circolazione dei dati personali. In effetti, tutti i (differenti) presupposti di liceità dei dati personali sono connotati in termini di *finalità* del trattamento (esecuzione di un contratto[4], adempimento di un obbligo legale[5], salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica[6]), ivi compreso il meccanismo del previo consenso, che

2. Cfr. l'art. 6, comma 1, lett. f) del GDPR, ai sensi del quale è lecito "il trattamento [quando] è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore".

3. Infatti, ai sensi del combinato disposto tra l'art. 6, comma 1, lett. f), l'art. 6, comma 3, lett. b) e l'art. 2-ter, comma 1 del Codice privacy, la base giuridica del trattamento di dati necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento", è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, da una norma di regolamento.

4. Cfr. l'art. 6, comma 1, lett. b) del GDPR.

5. Cfr. l'art. 6, comma 1, lett. c) del GDPR.

6. Cfr. l'art. 6, comma 1, lett. d) del GDPR.

infatti non costituisce una delega in bianco, ma va espresso "per una o più specifiche *finalità*"[7], che condizionano la liceità di ogni successivo uso.

Tuttavia – e qui sta la differenza, sulle cui conseguenze vorremmo riflettere – il soggetto di diritto comune dispone della possibilità (e dell'autonomia) di scegliere e determinare le finalità rispetto alle quali raccogliere il consenso presso dell'interessato. Diversamente, al soggetto che raccolga dati personali in vista dell'esercizio di un compito di interesse pubblico, questo spazio di manovra è del tutto precluso, sì che per esso (diversamente che per i soggetti di diritto comune) il principio/vincolo di finalità opera in modo più stringente, poiché – in modo del tutto fisiologico rispetto allo statuto della funzione amministrativa – la finalità risulta integralmente etero-determinata.

Il framework asimmetrico (tra titolari che esercitano *funzioni pubbliche* e titolari che si determinano *autonomamente*) così disegnato dal GDPR comporta (insieme ad altri fattori, di cui si dirà in seguito) una serie di effetti sulla concreta praticabilità della BDA/ML nell'ambito del settore pubblico, di cui si forniranno alcuni esempi concreti.

Per comodità espositiva, tratteremo il tema distinguendo il caso del soggetto pubblico (*rectius*, del titolare del trattamento "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri"[8]) come *fornitore* di dati personali, dal caso del soggetto pubblico quale *fruitore* di dati personali, in ottica di BDA/ML.

2. *Seconda premessa: principio di finalità e logica della BDA/ML*

Prima di procedere è però necessario introdurre un secondo ordine di considerazioni, utile ad evidenziare la tendenziale *incompatibilità* tra le logiche sottese alla BDA/ML e il principio di finalità (cardine del modello di tutela dei dati personali, in particolare nel contesto eurounitario). Il principio di finalità, infatti, è funzionale a garantire l'autonomia e/o il controllo da parte dell'interessato sull'uso dei dati da parte dei titolari del trattamento. Ciò che presuppone che l'interessato (o l'autorità di controllo) sia in condizioni di verificare che il trattamento sia funzionalmente connesso con la specifica finalità per la quale è stato fornito il consenso (o che sorregge la funzione pubblica, etc.), e che tale connessione sia mantenuta anche in seguito (in caso di trattamenti ulteriori). Tuttavia, le logiche del

7. Cfr. l'art. 6, comma 1, lett. a) del GDPR.
8. Cfr. l'art. 6, comma 1, lett. e) del GDPR.

BDA/ML entrano in conflitto con questo modello di tutela, dal momento che loro caratteristica precipua è quella di consentire l'emersione di conoscenza nuova ed *inattesa*, a partire dalla rilevazione di correlazioni/interrelazioni non immediatamente evidenti. Ciò comporta la radicale imprevedibilità dell'uso dei dati, sia con riferimento alla tipologia di trattamento, sia con riferimento alla finalità cui tale uso può in seguito risultare utile/funzionale[9]. L'avvento di queste tecniche di elaborazione dei dati mette in crisi il principio di finalità, che infatti da più parti è ritenuto non più idoneo quale istituto a tutela dell'interessato, in ragione – essenzialmente – della sua ineffettività[10]. Questa osservazione offre molte ragioni di perplessità circa l'impianto della disciplina eurounitaria (utili ed opportune *de jure condendo*), che in questa sede è doveroso richiamare[11], ma che non costituiscono l'oggetto delle nostre riflessioni. A noi interessa piuttosto evidenziare – de *jure condito* – come questa incompatibilità *di fondo* tra principio di finalità e logiche della BDA/ML interagisca con il framework asimmetrico di cui si è detto sopra. Come vedremo, la maggiore cogenza del principio di finalità nell'ambito dei trattamenti finalizzati all'esercizio di funzioni pubbliche determina alcuni effetti (enfatizzati anche da alcune scelte in sede di applicazione/completamento del quadro normativo eurounitario in sede nazionale) che amplificano la distanza (in termini di concreta

9. "If the reframing of consent in data protection rules has been instrumental in ensuring the continuous enhancement of the expression of user autonomy and control, new technologies are challenging its limits. There is growing skepticism over the efficiency of consent as a pervasive legal ground for legitimate personal data processing. The design of algorithmic data processing makes the unpredictable and even unimaginable use of data a feature, not a bug, which is directly at odds with the rights and obligations depicted in data protection rights and obligations such as the purpose specification obligation. How can explicit (or even informed) consent be given for specified data processing purposes when the process itself is not transparent or when the purpose is impossible to predict, specify, and explain *ex ante*?", così A. Giannopoulou, *Algorithmic systems: the consent is in the detail?*, in *Internet Policy Review*, 2000, 9(1), 3; *adde* M.L. Jones - E. Edenberg - E. Kaufman, *AI and the Ethics of Automating Consent*, in *IEEE Security & Privacy*, 2018, 16(3), 64 ss.

10. Cfr. L. Edwards - M. Veale, *Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?*, in *IEEE Security & Privacy*, 16(3), 2018, 46 ss.; D. Kamarinou - C. Millard - J. Singh, *Machine learning with personal data*, in *Queen Mary School of Law Legal Studies,* Research Paper n. 247/2016; M.S. Gal, *Algorithmic Challenges to Autonomous Choice*, in *Michigan Telecommunications and Technology Law Review*, 2018, 25(1), 59 ss.

11. Cfr. A. Mantelero, *Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework*, in *Computer Law & Security Review*, 2017, 5, 584 ss.

praticabilità) tra settore pubblico e settore privato. In sintesi, tali effetti paiono essere anche la conseguenza del diverso *tasso di ineffettività* del principio di finalità (per contrasto con le logiche della BDA/ML) che connota il settore pubblico rispetto a quello privato. Il primo, infatti, è oggetto di procedure di controllo più sistematiche e pervasive, ciò che determina un *maggior grado di effettività* del principio di finalità, con la conseguenza (come vedremo) che la realizzazione di servizi, procedure, e funzioni basati sul BDA/ML incontra ostacoli molto severi.

3. *L'amministrazione come fornitore di dati personali*

Il principio di finalità osta, in tutta evidenza, a che un'amministrazione possa – di propria iniziativa – rendere disponibili a soggetti terzi i dati personali che ha raccolto o che conserva per fini istituzionali, a meno che tale trattamento (la comunicazione, ovvero la diffusione) non sia espressamente prevista dalla legge. Simili previsioni di legge sono ricorrenti, in effetti, per quanto concerne la comunicazione di dati personali *tra amministrazioni*, e di questo aspetto ci occuperemo nel prossimo paragrafo. Per quanto concerne invece la comunicazione all'esterno del settore pubblico (o, *rectius*, al di fuori del perimetro dell'esercizio delle funzioni pubbliche), viene in rilievo una specifica categoria di dati personali che, proprio per effetto di specifiche previsioni legislative, possono essere rese conoscibili a chiunque. Si tratta di quel particolare sottoinsieme di dati personali che l'ordinamento ritiene di rendere conoscibili a chiunque, a fini di *trasparenza*; ossia, per assicurare l'accesso a quelle informazioni mediante la cui conoscenza i cittadini sono posti nella condizione di *comprendere* l'organizzazione, le azioni e le scelte effettuate dei poteri pubblici, al fine di operare quel controllo diffuso che è risvolto essenziale del principio democratico[12]. Lo stesso GDPR contempla questa categoria di dati, sebbene rimetta la determinazione della ampiezza e della consistenza, ed il relativo regime di accessibilità generalizzata, alla competenza del legislatore nazionale[13]. In questo modo, mentre il regime di tutela dei dati personali è

12. Cfr. F. Merloni, *Trasparenza delle istituzioni e principio democratico*, in F. Merloni (a cura di), *La trasparenza amministrativa*, Milano, 2008, 9 ss.; E. Carloni, *La "casa di vetro" e le riforme. Modelli e paradossi della trasparenza amministrativa*, in *Dir. Pubbl.*, 2009, 779 ss.

13. Cfr. l'art. 86 del GDPR, che recita "I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione

(sarebbe?) uniforme a livello UE, vi sono invece tanti (differenti) regimi di accesso ai dati personali quante sono le legislazioni nazionali che operano in concreto il bilanciamento autorizzato dall'art. 86 del GDPR[14].

Nell'ordinamento nazionale italiano, vi sono due principali istituti giuridici differenti che realizzano tale bilanciamento, e che pertanto concorrono a determinare il sottoinsieme di dati personali detenuti dai soggetti pubblici (o da chi eserciti una funzione pubblica) che possono essere fruiti all'esterno, da parte di soggetti terzi. Si tratta in particolare dei dati personali che debbono essere obbligatoriamente pubblicati sui siti delle amministrazioni pubbliche per effetto delle previsioni del d.lgs. n. 33/2013 ("Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"), e che pertanto come tali sono fruibili (o, quantomeno, accessibili) da parte di chiunque; si tratta poi dei dati personali la cui *disclosure* consegua ad una richiesta di accesso civico generalizzato di cui all'art. 5, comma 2 del medesimo decreto legislativo (richiesta potenzialmente attivabile da chiunque).

Questo sottoinsieme di dati personali può essere oggetto di trattamenti (da parte di terzi che vi accedono o ne fruiscono) secondo la logica della BDA/ML? Una prima risposta affermativa potrebbe dedursi dalla chiara statuizione di cui all'art. 3 del decreto "trasparenza", che sancisce (anche) il diritto a riutilizzare i dati resi pubblici mediante pubblicazione o mediante accesso generalizzato[15]. Come vedremo di qui a breve, però, le cose non stanno esattamente in questi termini.

di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo *conformemente al diritto* dell'Unione o *degli Stati membri* cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento" (corsivo aggiunto).

14. Per quanto concerne bilanciamento asimmetrico tra tutela dei dati personali e diritto alla trasparenza, che caratterizza l'assetto normativo all'incrocio tra ordinamento UE e ordinamenti nazionali degli stati membri, sia consentito rinviare a B. Ponti, *Il luogo adatto dove bilanciare. Il "posizionamento" del diritto alla riservatezza e alla tutela dei dati personali vs il diritto alla trasparenza nella sentenza n. 20/2019*, in *Istituzioni del federalimo*, 2019, 2, 525 ss.

15. Cfr. l'art. 3, comma 1 del d.lgs. 33/2013, che recita "Tutti i documenti, le informazioni e i dati oggetto di accesso civico, ivi compresi quelli oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell'articolo 7".

3.1 *I dati personali pubblici resi disponibili secondo il meccanismo della pubblicazione/diffusione*

Cominciando dai dati personali oggetto di pubblicazione obbligatoria, occorre considerare che le risposte al quesito circa la effettiva riutilizzabilità dei dati personali pubblicati e diffusi ai sensi del decreto trasparenza, alla luce della disciplina di tutela dei dati personali, sono mutate nel tempo, al mutare del quadro normativo di riferimento. In vigenza del precedente quadro normativo (costituito dalla direttiva 95/46/CE e dalla disciplina nazionale di recepimento, raccolta nel d.lgs. n. 196/2003, il cd. "Codice privacy"), le indicazioni formulate dall'autorità di settore miravano a contenere il problema "a valle" (ossia, in una fase procedurale successiva alla fuoriuscita dei dati personali determinata dall'adempimento dell'obbligo di pubblicazione). In particolare, l'approccio delle linee guida varate nel 2014 per fornire indicazioni alle amministrazioni[16] su come contemperare obblighi di pubblicazione e regime di tutela dei dati personali tendeva a scaricare sulle amministrazioni stesse (e non sui fruitori esterni) il compito di dare effettività al principio di finalità, al fine di contemperare il "diritto al riutilizzo" sancito dall'art. 3 del d.lgs. n. 33/2013 (e dal successivo art. 7) con i principi a tutela dei dati personali. Era dunque compito delle amministrazioni limitare (o addirittura proibire) la possibilità di (ri)utilizzo dei dati personali (pure) resi obbligatoriamente disponibili, a seguito di una "rigorosa valutazione di impatto in materia di protezione dei dati, al fine di ridurre il rischio di perdere il controllo sulle medesime informazioni o di dover far fronte a richieste di risarcimento del danno da parte degli interessati"[17]. Le linee guida costruivano quindi un meccanismo che tendeva a collocare il peso delle responsabilità per eventuali danni derivanti dalle attività di riutilizzo poste in essere dai terzi (anche quelle consistenti nell'applicazione della logica BDA/LM) anche sulle amministrazioni. Una soluzione di massima precauzione, anche se di dubbia efficacia, dal momento che le licenze in questione non avevano altro valore che ribadire obblighi e presupposti di liceità (gravanti sui terzi riutilizzatori) già imposti dall'ordinamento, e sembravano onerare le amministrazioni di

16. Cfr. le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati", adottate con provvedimento del 15 maggio 2014.

17. Cfr. *ivi*, parte I, par. 6. "Limiti al 'riutilizzo' di dati personali (artt. 4 e 7 del d. lgs. n. 33/2013)".

un compito impossibile da perseguire (quello di non perdere il controllo delle informazioni).

Qualcosa cambia con l'avvento del GDPR, che all'art. 5 ("Principi applicabili al trattamento dei dati personali") introduce il cd principio di responsabilizzazione, in base al quale è "il titolare del trattamento [che] è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)"[18]. In base a questo principio, la responsabilità per il mancato rispetto dei requisiti di liceità (ossia, il "il rispetto del paragrafo 1") ricade sul titolare del trattamento medesimo (ossia, sul soggetto che "determina le finalità e i mezzi del trattamento di dati personali"), così che lo schema disegnato dalle linee guida del 2014 pare perdere di mordente, risultando difficile chiamare a rispondere le amministrazioni per trattamenti di cui non risultano titolari (le p.a. essendo titolari del trattamento consistente nella pubblicazione, mentre i titolari dei trattamenti consistenti in eventuali riutilizzi di tali dati da parte di terzi sono appunto questi ultimi).

Forse non è casuale, dunque, che – una volta indebolita la possibilità di inibire "a valle" la possibilità di riutilizzo dei dati (personali) oggetto di pubblicazione obbligatoria – l'attenzione si sia spostata "a monte", ovvero sul perimetro dei dati oggetto di pubblicazione obbligatoria (oggetto, cioè, di fuoriuscita). Come noto, il *casus belli* è stato rappresentato dall'estensione (nel 2016[19]) a tutti i titolari di incarico dirigenziale degli obblighi di pubblicità reddituale e patrimoniale già previsti nel 2013 in capo ai titolari degli organi di indirizzo politico. La nota sentenza della Corte costituzionale, chiamata dal T.A.R Lazio a verificare la compatibilità di tale disciplina con plurimi principi costituzionali e eurounitari, è rilevante sotto molteplici aspetti[20], non ultimo il fatto che il modello di pubblicità/trasparenza

18. Cfr. l'art. 5, comma 2 del GDPR.

19. L'ampliamento dell'ambito soggettivo di applicazione degli obblighi di pubblicità relativa ai dati personali patrimoniali e reddituali, con l'inclusione di tutti i titolari di incarico dirigenziale avviene ad opera del d.lgs. n. 97/2016, adottato in attuazione della delega contenuta nella legge 124/2015, cd. legge "Madia".

20. Nella sentenza 19/2020 la Corte, infatti, ritorna sulla svolta operata con la precedente sentenza n. 269/2017, e relativa al trattamento da riservare all'incidente di costituzionalità nel caso in cui un medesimo diritto riceva protezione (o copertura) sia da parte del diritto costituzionale interno, sia da parte della Carta dei diritti fondamentali dell'Unione europea, ciò che ha comprensibilmente attirato l'attenzione dei commentatori, interessati a verificare se ed in che misura il Giudice delle leggi avrebbe confermato gli approdi di quella epocale pronuncia del 2017; cfr. *ex multis* A. Ruggeri, *La Consulta rimette a punto i rapporti tra diritto eurounitario e diritto intero con una pronunzia in chiaroscuro (a prima lettura di Corte cost. n. 20 del 2019)*, in *Consulta Online*, 23 febbraio 2019; O. Pollicino - G. Repetto, *Not to be Pushed Aside: the Italian Constitutional Court and the European Court*

adottato con il d.lgs. n. 33/2013 non ne è uscito stravolto sotto il profilo oggettivo, ma solo limitato quanto alla sua applicazione soggettiva[21]. Ciò che qui interessa sottolineare, però, è che l'esistenza e l'affermazione delle tecniche e le logiche della BDA/ML hanno giocato un ruolo non secondario nell'indirizzare tanto il giudice remittente, quanto la Consulta, in quella parte del giudizio in cui il regime delle pubblicità dei dati reddituali e patrimoniali è stato valutato come sproporzionato. Già il T.A.R. (in sede di rimessione) aveva evidenziato che la mole enorme di dati resi disponibili fosse inintellegibile (e quindi, scarsamente utile proprio a fini di trasparenza) dalla generalità dei cittadini, il cui gran numero risulta privo di quella capacità di lettura che è propria invece di quei "soggetti complessi a vario titolo operanti nell'ordinamento vigente, che, *essendo in possesso di strumenti idonei a decrittare importanti masse di informazioni*, risultano, a legislazione vigente […] allo stato i soli in grado di trarre dalle stesse conclusioni coerenti con quanto complessivamente reso disponibile e con gli obiettivi propri della legislazione di cui trattasi"[22]. Argomentazione ripresa e confermata dalla Consulta, che ha notato come "la pubblicazione di quantità così massicce di dati, infatti, non agevola affatto la ricerca di quelli più significativi a determinati fini (nel nostro caso particolare, ai fini di informazione veritiera, anche a scopi anticorruttivi) se non siano utilizzati efficaci strumenti di elaborazione, che non è ragionevole supporre siano a disposizione dei singoli cittadini.", soggiungendo poco oltre il rischio "di generare 'opacità per confusione', proprio per l'irragionevole mancata selezione, a monte, delle informazioni più idonee al perseguimento dei legittimi obiettivi perseguiti"[23]. Come si vede, proprio l'esistenza di strumenti e tecniche idonei a estrarre conoscenza da una massa di informazione altrimenti illeggibile (e confusa), strumenti però indisponibili alla generalità dei cittadini, ma concentrati in pochi soggetti "complessi" comporta una

of Justice, in *VerfBlog*, 27 febbraio 2019, G. Bronzini, *La sentenza n. 20/2019 della Corte costituzionale italiana: verso un riavvicinamento all'orientamento della Corte di giustizia?*, in *Questione Giustizia*, 4 marzo 2019.

21. Cfr. B. Ponti, *Il luogo adatto dove bilanciare*, cit., 542-543. Per altro, il legislatore (d.l. n. 162/2019, art. 1, comma 7) ha risposto all'appello della Corte a rivedere in modo organico i termini del bilanciamento, ed ha formulato a questo fino alcuni criteri direttivi da tradurre in un regolamento governativo i cui termini di approvazioni e dapprima fissati al 31.12.2020 sono stati in seguito prorogati al 30.04.2021).

22. Così T.A.R. Lazio (sezione I quater), ordinanza del 19 settembre 2017, n. 9828 (corsivo mio).

23. Corte Cost., sentenza 27 febbraio 2019, n. 20, p.to 5.3.1. *Cons. dir.*

censura nei confronti del meccanismo di "fuoriuscita" dei dati personali così congegnato. V'è, in queste considerazioni, una prefigurazione del potere conoscitivo di "pochi soggetti complessi" (quella che in letteratura è definita anche *digital dominance*[24]) che pare alimentarsi proprio della rottura/superamento del principio di finalità. Non a caso, il giudice pare prediligere invece un meccanismo che selezioni "a monte" le informazioni utili e finalizzate a realizzare la trasparenza: un approccio questo che appare pienamente coerente con il principio di finalità.

3.2 *I dati personali pubblici resi disponibili secondo il meccanismo dell'accesso generalizzato*

Ancora più significativo è il caso dell'altro meccanismo di fuoriuscita di dati personali, quello che consegue ad un accesso Foia. La disciplina legislativa contempla esplicitamente la circostanza che i dati personali possa essere oggetto di *disclosure*, sia perché l'accesso civico generalizzato di cui all'art. 5, comma 2 del d.lgs. n. 33/2013 (come risultante dalle modifiche apportate dal d.lgs. n. 97/2016) si applica "a tutti dati e i documenti detenuti dalla pubblica amministrazione", sia perché l'art. 5-bis, comma 2 contempla la possibilità di rifiutare l'accesso qualora il diniego sia necessario per evitare un pregiudizio concreto all'interesse privato alla "protezione dei dati personali, in conformità con la disciplina legislativa in materia": ciò comporta che in assenza di tale pregiudizio concreto il dato personale è (invece) accessibile. Questo quantomeno *in teoria*. Nella prassi, invece, si è affermato un indirizzo interpretativo che ha condotto, nella stragrande maggioranza dei casi, ad un diniego di accesso a dati personali, anche quando si è trattato di dati personali particolarmente connessi all'esercizio di una funzione pubblica (e quindi, più funzionali di altri alla finalità della trasparenza). Ciò che qui interessa sottolineare, tuttavia, non è tanto la proporzione dei dinieghi a fronte degli accoglimenti (comunque significativa), quanto le ragioni addotte per motivare tali dinieghi. Va notato che tali motivazioni sono elaborate essenzialmente dal Garante privacy, che deve essere sempre sentito nelle procedure di ricorso in sede amministrativa che abbiano ad oggetto dati personali. Orbene, nella più larga maggioranza dei casi il parere del Garante (a supporto dei dinieghi di accesso) delinea il seguente percorso argomentativo: quando un dato personale è oggetto di *disclosure* a seguito di una richiesta di accesso civico generalizzato, quel dato acquista il regime

24. Cfr. M. Moore - D. Tambini (a cura di), *Digital dominance: the power of Google, Amazon, Facebook, and Apple*, New York, Oxford University Press, 2018.

del dato pubblico, in quanto conoscibile da chiunque; in conseguenza di questo *status*, il dato personale può essere riutilizzato (ai sensi della disciplina pertinente); poiché al momento della richiesta di accesso non può essere apprezzato in quali contesti tale riutilizzo potrebbe essere effettuato (in seguito) né a quali effetti esso potrebbe dare luogo, e poiché tali effetti potrebbero essere anche di carattere pregiudizievole per l'interessato, allora per evitare questo potenziale pregiudizio l'acceso viene rifiutato[25]. Dunque, la non prevedibilità degli effetti del riutilizzo (ossia, il carattere distintivo della logica sottesa alla BDA/ML e che si pone in antitesi al principio di finalità) opera (nell'interpretazione del Garante) come un rubinetto che tende a "chiudere" il flusso di dati personali all'esterno del soggetto pubblico. Anche in questo caso, dunque, emerge l'incompatibilità tra il meccanismo di tutela dei dati personali (prevedibilità della finalità/tipologia d'uso, così da poterne apprezzare la "pericolosità") e logica della BDA/ML, con la prima che opera al fine di evitare la concreta praticabilità della seconda.

Va sottolineato che in entrambi i casi qui sopra rappresentati, la limitazione o l'esclusione della fuoriuscita di dati personali finisce per frustrare anche la praticabilità di soluzioni basate su BDA/ML che abbiano come obiettivo proprio la trasparenza, e che pertanto risulterebbero pienamente in linea con il principio di finalità[26]. La minimizzazione del rischio (potenzialmente derivante da usi non preventivabili e pregiudizievoli) comporta anche la preclusione alle potenziali opportunità. Tale approccio – pur comprensibile, soprattutto quando proposto dall'autorità che ha come (unica) missione istituzionale quella di tutelare i dati personali – appare però non pienamente allineato al quadro normativo eurounitario, che mediante l'esplicitazione del principio di responsabilizzazione sembra prediligere

25. È ricorrente, nei pareri del Garante sulle richieste di accesso civico "Foia", la seguente formula: "si ritiene che l'ostensione dei dati e delle informazioni personali oggetto dell'istanza di accesso civico – considerando che «Tutti i documenti, le informazioni e i dati oggetto di accesso civico […] sono pubblici e chiunque ha diritto di conoscerli, di fruirne gratuitamente, e di utilizzarli e riutilizzarli ai sensi dell´articolo 7» (art. 3, comma 1, del d. lgs. n. 33/2013), sebbene il loro ulteriore trattamento vada in ogni caso effettuato nel rispetto dei limiti derivanti dalla normativa in materia di trattamento dei dati personali – sia suscettibile di determinare, a seconda dei casi e del contesto in cui possono essere utilizzati da terzi, proprio quel pregiudizio concreto alla tutela della protezione dei dati personali previsto dall´art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013" (*ex multis* cfr. Garante privacy, parere del 10 aprile 2017, n. 190).

26. Quanto all'esercizio del diritto al riutilizzo dei dati pubblici, come strumentale alla realizzazione della trasparenza, sia consentito rinviare a B. Ponti, *La mediazione informativa nel regime giuridico della trasparenza: spunti ricostruttivi*, in *Diritto dell'informazione e dell'informatica*, 2019, 383 ss.

modelli regolatori diversi da quelli integralmente fondati sull'esigenza di prevenire ogni possibile rischio, anche a costo di impedire la concreta praticabilità di soluzioni che – quantomeno in certi casi – potrebbero risultare non solo utili, ma anche coerenti con il principio di finalità.

4. *L'amministrazione come fruitore di dati personali*

Il secondo profilo che vorremmo rapidamente indagare è quello della praticabilità di soluzioni basate sulla logica BDA/LM applicata (anche) a dati personali raccolti e detenuti dall'amministrazione, questa volta da parte della stessa amministrazione. Si tratta di un profilo di enorme rilievo, anche in considerazione della mole di dati personali detenuti dal settore pubblico, complessivamente inteso. Il vincolo principale – come già sottolineato – è quello del principio di finalità come connesso a quello di legalità/funzionalizzazione dell'azione amministrativa. I dati personali (già detenuti) possono essere (ri)utilizzati solo per finalità che siano le medesime che ne avevano giustificato la raccolta, ovvero per ulteriori finalità che siano valutate come "compatibili" con le prime[27]. Le finalità sono quelle definite (in termini eteronomi) dal quadro normativo che attribuisce poteri e compiti di interesse pubblico. Pertanto, l'amministrazione subisce (fisiologicamente) questo doppio vincolo: riceve le finalità dall'ordinamento (principio di legalità/attribuzione) e può (ri)utilizzare i dati solo per trattamenti che siano necessari per conseguire tali finalità (o finalità con queste compatibili). In via di prima approssimazione, dunque, si potrebbe ritenere che una soluzione BDA/LM (che contempli anche il trattamento di dati personali) che sia progettata per realizzare finalità identiche o compatibili con quelle affidate all'amministrazione costituisca una strada astrattamente percorribile.

L'approfondimento della normativa (eurounitaria e nazionale), nonché della prassi maturata negli ultimi anni, ci consente però di apprezzare un quadro regolatorio affatto complesso, nel quale le condizioni effettive di praticabilità di soluzioni BDA/ML risultano particolarmente sacrificate.

Vediamone le ragioni.

4.1 *Il quadro normativo*

In primo luogo, occorre considerare che il patrimonio informativo è distribuito tra differenti amministrazioni ed enti pubblici; con riferimento

27. Cfr. l'art. 6, comma 4 del GDPR.

a quella parte costituta da dati personali (largamente maggioritaria), tale (accentuato) decentramento non costituisce affatto un accidente della storia, ma è piuttosto il frutto di una precisa scelta di politica del diritto, maturata nel corso degli anni settanta del secolo scorso, come risposta "di sistema" ai pericoli derivanti dalla concentrazione di potere conoscitivo connessa all'emergere delle tecnologie di memorizzazione ed elaborazione dei dati. Quella scelta era il frutto di riflessioni consapevoli e particolarmente avanzate[28], e non è nostra intenzione metterla in discussione in termini retrospettivi (tutt'altro). Tuttavia, occorre pure fare i conti con alcuni effetti a lungo termine di quella scelta, e che hanno come punto di caduta il framework asimmetrico di cui s'è detto in apertura. Mentre le banche dati di dati personali sono strutturalmente *distribuite* all'interno del settore pubblico, gli attori privati (*rectius*, quei soggetti "complessi" e dominanti, cui faceva riferimento il T.A.R. Lazio nel 2017) possono procedere alla loro illimitata *concentrazione*, e proprio sulla base del principio del consenso (e delle sue ormai evidenti debolezze). Cosa comporti questo in termini di differente praticabilità (nei due contesti) di soluzioni basate su BDA/ML non è difficile immaginarlo.

In termini concreti, poiché i dati personali sono "distribuiti" può accadere (anzi, è l'occorrenza fisiologicamente largamente prevalente) che lo sviluppo di una soluzione di BDA/ML necessiti della integrazione tra banche dati differenti e diversamente dislocate, ossia di un trattamento preliminare: la comunicazione/duplicazione della banca dati. Su questo punto, il legislatore nazionale ha in parte utilizzato gli spazi regolatori aperti dal GDPR, che consente di mantenere o introdurre requisiti e misure ulteriori a garanzia della liceità e della correttezza dei trattamenti[29]. In particolare, il Codice della privacy, come da ultimo modificato per adeguarsi al GDPR, prevede che se il trattamento è effettuato da una amministrazione diversa da quella che ne è titolare, la comunicazione dei dati da parte dell'amministrazione titolare dei dati è ammessa solo se prevista dalla legge. Se manca tale previsione nella legge, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali, e può essere iniziata se è decorso il termine di quarantacinque giorni dalla

28. Su tutti, lo studio precursore di S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

29. Cfr. l'art. 6, comma 2 del GDPR, che consente di introdurre requisiti e condizioni ulteriori proprio con riferimento ai trattamenti necessari per lo svolgimento di compiti di interesse pubblico.

relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati[30]. Consideriamo che l'autorizzazione legislativa sarebbe comunque necessaria nel caso di trattamenti (ivi compresa la comunicazione tra amministrazioni di dati personali) con finalità non compatibili con quella originaria. Ciò comporta che il legislatore nazionale ha (in effetti) introdotto un obbligo di segnalazione al Garante per tutti i casi in cui la comunicazione/il trasferimento dei dati dall'amministrazione che ne è titolare a quella che intende effettuarne il riutilizzo sia funzionale ad un trattamento che è stato valutato (dalle stesse amministrazioni coinvolte) come compatibile con la finalità originari. L'obbligo di segnalazione consente al Garante di indicare eventuali misure a garanzia degli interessati, ma costituisce anche occasione per una valutazione di secondo grado circa la compatibilità tra il nuovo trattamento e quello originario. Anche in questo caso, dunque, viene messa in opera una soluzione volta ad accrescere il tasso di effettività di principio di finalità, una misura che lascia intendere che il principio di responsabilizzazione ha minore rilevanza, quando si tratta di trattamenti posti in essere da soggetti che esercitano poteri pubblici o funzioni/compiti di interesse pubblico. L'asimmetria del framework regolatorio ne risulta così ulteriormente rafforzata.

4.2 *La prassi*

Un secondo elemento che occorre considerare è l'interpretazione dei principi rilevanti in materia elaborata dall'autorità di garanzia, proprio con riferimento alle tecniche di trattamento dei dati che fanno riferimento alle logiche della BDA/ML. Si è già notato che il Garante privacy ha una considerevole voce in capitolo (da giocarsi generalmente in via preventiva, a dispetto del principio di responsabilizzazione), pertanto questo fattore ha un peso decisivo nel definire i margini di concreta praticabilità di queste tipologie di trattamento da parte dei soggetti pubblici.

Le decisioni maturate nel corso degli ultimi anni sono molteplici, e di notevole rilievo, sebbene non tutte comparabili tra loro. Ad esempio, il caso del sistema "SAVIO" – elaborato dall'INPS al fine di concentrare le visite fiscali sui certificati di malattia che presentassero un profilo di più elevato rischio di comportamento anomalo e quindi più probabilmente scorretto o fraudolento (che certamente si basava sul procedure di BDA/ML quali

30. Cfr. l'art. 2-ter, comma 2 del d.lgs. n. 196/2006 (Codice della privacy) così come introdotto dal d.lgs. n. 101/2018.

il *data-mining*), sistema che è stato valutato alla luce del quadro normativo allora vigente (e quindi precedente all'entrata in vigore del GDPR) – presentava significative peculiarità, configurandosi come trattamento integralmente automatizzato, volto alla profilazione (art. 22 GDPR) e che utilizzava dati idonei a rivelare lo stato di salute (art. 9 GDPR). Un insieme di elementi che rendono indispensabile non solo una specifica autorizzazione di rango legislativo (che mancava, e manca tutt'ora), ma anche la previsione di misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato. In questo senso, i provvedimenti assunti da Garante[31], e rivolti a interrompere l'uso del sistema (ed anche a sanzionare l'amministrazione) appaiono del tutto aderenti/vincolati dal quadro normativo.

Vi sono tuttavia altri casi in cui – anche in assenza di alcuni di questi elementi – il Garante segnala la tendenza ad interpretare le soluzioni basate sul *machine learning* come comunque incompatibili con il principio di finalità, dal momento la loro applicazione non consente di apprezzare in anticipo i criteri, le modalità e gli esiti del trattamento. Un caso di scuola è rappresentato dalla prolungata interlocuzione tra il Garante e l'Agenzia delle Entrate con riferimento all'uso dei dati integrati nell'Anagrafe rapporti finanziari al fine profilare il rischio di evasione fiscale, così da indirizzare i controlli in modo più efficace. Una interlocuzione affatto significativa, poiché per un verso testimonia in concreto come le logiche del principio di finalità (così come interpretate da Garante) risultino incompatibili con quelle di correlazione statistica che sono proprie del ML[32]; dall'altro, indicano come in questo caso (ma analogo è il caso

31. Cfr. Garante privacy, ordinanza d'ingiunzione 29 novembre 2018, n. 492.

32. "Prendiamo ad esempio la vicenda dell'anagrafe dei rapporti e dei conti finanziari dove, dal 2011, accedono i dati relativi ai saldi iniziali, alla giacenza media e ai saldi finali di ogni conto, con i relativi dati anagrafici. In un provvedimento del 17 aprile 2012 il Garante ha stabilito che, per consentire l'utilizzo dei dati, l'Agenzia dovesse sottoporre al Garante stesso preliminarmente i criteri per l'elaborazione delle liste di contribuenti a rischio di evasione. I criteri di profilazione, tuttavia, sono l'esito e non il presupposto dell'analisi dei dati. Se i dati rivelano correlazioni significative tra alcune caratteristiche personali (ad esempio, uno scostamento significativo tra le giacenze medie sul conto e i dati della dichiarazione, magari combinati in modo non lineare con tutte le altre caratteristiche individuali) e i comportamenti a rischio (ad esempio la presenza di un'evasione accertata e definita), allora quelle caratteristiche personali diventano un criterio di rischio. Ma queste correlazioni sono rivelate dai dati, non decidibili a priori. E, soprattutto, a posteriori queste correlazioni possono essere difficilmente spiegabili o comprensibili se non, appunto, come regolarità statistiche. Venendo alla sperimentazione, la questione diventa quindi la seguente: il Garante accetterebbe di trovarsi di fronte un insieme di criteri di individuazione dei diversi gradi di rischio che non sono spiegabili e valutabili se non sulla base degli esiti

INPS/SAVIO) l'interlocuzione tra Amministrazione e Garante ha come esito lo scaricare sul legislatore il compito di sciogliere i nodi controversi (liceità del trattamento, e della profilazione, tipologia dei dati da trattare, logiche del trattamento, etc.)[33]. Ciò che – per un verso – conferma (e, semmai, consolida ulteriormente) il principio di stretta legalità che regge il trattamento dei dati personali da parte dei soggetti pubblici; per altro verso, testimonia della difficile praticabilità tanto della sperimentazione, quanto della messa a regime di queste soluzioni, costrette a fare i conti con quadro regolatorio che, quando non apertamente non ostile[34], si rivela comunque estremamente rigido (in ragione del ruolo eminente svolto proprio dal legislatore).

A contrario, è significativo richiamare la recente esperienza della Regione Veneto che, per monitorare e tracciare la diffusione del virus così ed intervenire in modo mirato per contenere i focolai e circoscrivere il

puramente o almeno prevalentemente statistici dell'incrocio dei dati avvenuto a monte? La risposta affermativa implica la rinuncia del Garante a porre in questione la logicità astratta di quei criteri (al limite andrebbe valutata la metodologia statistica utilizzata, ma è opportuno che questa funzione sia svolta dal Garante della privacy?). La risposta negativa implica l'impossibilità di arrivare ai criteri attraverso un'analisi approfondita dei dati", così A. Santoro, *Lotta all'evasione e privacy dei cittadini. Replica al Presidente del Garante privacy*, in *lavoce.info*, 4.10.2019, testo disponibile al sito www.lavoce.info.

33. La disciplina legislativa istitutiva dell'Anagrafe dei rapporti presso l'Agenzia delle Entrate, finalizzata a integrare una serie di informazioni provenienti da fonti differenti, così da consentire un'analisi del rischio di evasione ed elusione fiscale, risale al 2011 (art. 11 del d.l. n. 201/2011, il cosiddetto "salva Italia"), è stata oggetto di successive modifiche in quattro occasioni, anche al fine di adeguarsi alle indicazioni formulate nei pareri espressi dal Garante privacy, che in varie occasioni (a cominciare dal parere n. 145 del 17 aprile 2012) aveva frustrato i tentativi di dare seguito alla realizzazione di soluzioni volte a profilare il rischio di comportamenti fiscalmente scorretti. Da ultimo, anche la legge di bilancio per il 2020 è intervenuta nel tentativo di rimuovere gli ostacoli (connessi al regime di tutela dei dati personali, ed emersi nel corso della prolungata interlocuzione tra Agenzia e Garante) che ancora si frapponevano alla realizzazione di soluzioni di analisi dei dati basate sul ML, e volte a profilare il rischio di evasione (cfr. l. n. 160/2029, art. 1, commi 681-686).

34. Un'ulteriore caso degno di nota è rappresentato dalle notevoli difficoltà incontrate in sede di elaborazione ed adozione del Piano statistico nazionale (PSN) 2017-2019 ed aggiornamento 2019, riconducibili in larga misura all'implementazione da parte dell'Istat di metodologie di estrazione ed aggregazione dei dati volte a semplificare le metodologie di raccolta, evitare duplicazioni, favorire la realizzazione di lavori statistici anche a partire dalla raccolta e l'integrazione di microdati da fonti amministrative, ciò che ha suscitato le perplessità del Garante, che ha più volte protratto l'istruttoria si punti qualificanti del piano. Per farse un'idea, si vedano i provvedimenti del Garante del 9 maggio 2018 e del 13 febbraio 2019.

contagio, ha predisposto a tempo di record una soluzione basata sull'incrocio di tre diverse banche dati (l'anagrafe sanitaria, che fornisce gli indirizzi dei contagiati e dei conviventi; quella dei dipendenti del sistema sanitario; nonché il database di Veneto Lavoro, l'agenzia regionale che raccoglie i dati di tutti i dipendenti delle aziende e dei datori di lavoro). Una soluzione che ha dimostrato una notevole efficacia, che ha supportato la politica una politica di prevenzione e contenimento del contagio di successo[35]. Come testimoniato dagli stessi protagonisti della vicenda, la predisposizione del "cruscotto" a supporto delle attività di biosorveglianza è stata possibile solo "forzando" la disciplina a tutela dei dati personali[36], quantomeno finché non è intervenuto il legislatore dell'emergenza ad allentarne le maglie[37].

Non è quindi un caso che la recente indagine conoscitiva congiunta da parte di tre autorità indipendenti sul tema dei *Big Data*[38] si occupi solo in termini estremamente marginali del settore pubblico (per altro, proprio a carico della parte curata da Garante privacy), considerato un ambito di scarso rilievo per la conoscenza del fenomeno. Si può inoltre notare che solo a marzo del 2018 il governo ha lanciato un'iniziativa per diffondere la consapevolezza delle opportunità della cd. Intelligenza Artificiale nel settore pubblico, iniziativa che (al di là della stesura di un sintetico *Libro Bianco*) non ha prodotto effetti significativi.

35. Per una illustrazione della piattaforma si veda l'articolo di *Engeneering* (la azienda produttrice del software) *#FASE 2: Engineering e l'analisi integrata dei dati per la protezione dei cittadini da Sars-Covid-2*, in www.eng.it, 2 maggio 2020. Vedi anche R. Luna, *I dati del virus, il Veneto e la piattaforma di cui abbiamo bisogno*, disponibile al sito www.repubblica.it, 2 maggio 2020.

36. «Inutile negarlo – riconosce Gubian [responsabile dell'unità operativa complessa dei sistemi informativi di Azienda Zero, l'ente sanitario cui fanno capo tutte le Asl del Veneto, *N.d.R.*] – in tempi normali non si sarebbero potute incrociare queste banche dati. L'abbiamo fatto nell'interesse superiore della salute pubblica, partendo dall'idea che al sistema di contrasto non debba sfuggire neppure un caso positivo perché potrebbe essere generatore di morti. È chiaro che finita l'ermergenza tutto dovrà rientrare», cfr. A. Pasualetto, *Coronavirus, Crisanti: «Così ho violato le regole sui tamponi e ho fatto bene»*, 1 giugno 2020, disponibile al sito www.corriere.it.

37. Per effetto delle disposizioni contenute nell'art. 14 del d.l. n. 14/2020, convertito in l. n. 6/2020.

38. Cfr. AGCM, Agcom, Garante privacy, Indagine conoscitiva sui *Big data*, 2019, disponibile al sito www.agcom.it.