

Rivista di diritto amministrativo

Pubblicata in internet all'indirizzo www.amministrativamente.com

Direzione scientifica
Gennaro Terracciano, Gabriella Mazzei

Direttore Responsabile
Marco Cardilli

Coordinamento Editoriale
Luigi Ferrara, Giuseppe Egidio Iacovino,
Carlo Rizzo, Francesco Rota, Valerio Sarcone

FASCICOLO N. 11-12/2018

estratto

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

Comitato scientifico

Salvatore Bonfiglio, Gianfranco D'Alessio, Gianluca Gardini, Francesco Merloni, Giuseppe Palma, Angelo Piazza, Alessandra Pioggia, Antonio Uricchio, Vincenzo Caputi Jambrenghi, Annamaria Angiuli, Helene Puliat, J. Sánchez-Mesa Martínez, Andry Matilla Correa.

Comitato dei referee

Gaetano Caputi, Marilena Rispoli, Luca Perfetti, Giuseppe Bettoni, Pier Paolo Forte, Ruggiero di Pace, Enrico Carloni, Stefano Gattamelata, Simonetta Pasqua, Guido Clemente di San Luca, Francesco Cardarelli, Anna Corrado, Fabrizio Cerioni, Gaetano Natullo, Paola Saracini, Mario Cerbone, Margherita Interlandi, Bruno Mercurio, Giuseppe Doria, Salvatore Villani.

Comitato editoriale

Laura Albano, Daniela Bolognino, Caterina Bova, Sergio Contessa, Ambrogio De Siano, Fortunato Gambardella, Flavio Genghi, Jakub Handrlica, Laura Letizia, Massimo Pellingra, Marcin Princ, Stenio Salzano, Francesco Soluri, Giuliano Taglianetti, Marco Tartaglione, Stefania Terracciano.

La tutela della privacy nello scambio di dati personali tra pubbliche amministrazioni

di Filippo Lorè

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

Sommario

1. La cornice normativa in materia di protezione dei dati personali; 2. La comunicazione delle banche dati tra pubbliche amministrazioni e i rischi legati alla protezione dei dati personali; 3. Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche.

Abstract

The control over the use of personal data constitutes the new challenge that awaits the public administration, exercised, between confidentiality, transparency and information security, by the person in charge of protection of personal data and other figures expressly provided for by the Digital Administration Code. And here the concept of privacy is enriched by its primordial meaning, until it finds full identity in the right to protection of personal data of every citizen. The data protection industry, like all new digital professions, requires a high level of training and continuous professional updating to identify and resolve the non-compliance with the legislation on personal data protection with organized and systematic criteria in order to optimize and harmonize the processes in order to identify good practices for compliance with privacy legislation.

In the first part of this work we tried to outline the path that the community legislator has taken with the introduction of the principles of accountability, privacy by design, privacy by default and the centrality of the person responsible for personal data protection.

In the second part, without pretension of exhaustiveness, we analyzed the activity of the Guarantor for the protection of personal data in one of its most important measures for the public sector: the methods of communication and exchange of databases between public offices.

In the third part, the energies were channeled to the identification of brief recommendations for public administrations, where the practical and theoretical aspects both play an important role in guaranteeing dynamism and competitiveness in a strategic vision that is in step with the times.

1. La cornice normativa in materia di protezione dei dati personali

Con l'entrata in vigore del Regolamento generale sulla protezione dei dati personali UE 2016/679 il 24 maggio e del D.Lgs n.101/2018 che ha adattato al Regolamento il Codice in materia di protezione dei dati personali, si definisce il nuovo approccio sotto il profilo della riservatezza e della protezione dei dati personali: ciò viene richiesto alle pubbliche amministrazione che, nell'assolvimento delle funzioni istituzionali, assumono le decisioni rilevanti in tema di trattamento di dati personali (titolari e responsabili del trattamento). È richiesto un atteggiamento proattivo, che, oltre ad assicurare il rispetto dei principi di protezione dati, e garantire, quindi, la conformità normativa, consideri la *data protection* materia prima dell'economia dell'informazione e della condivisione. Ciò implica un approccio sistemico nella gestione del dato personale attraverso l'adozione di misure giuridiche, organizzative e tecniche, che assicurino la protezione dei dati in ogni fase del trattamento.

Le recenti disposizioni introdotte dal legislatore europeo rappresentano un assoluto elemento di novità per gli Enti pubblici, i quali dovranno, a differenza di quello che accadeva nella Direttiva 95/46/CE, adottare misure di sicurezza specifiche (e non appropriate come avveniva in passato) e ponderare il livello di rischio che le operazioni di trattamento possono comportare[1]. Tale diversa prospettiva richiede alle pubbliche amministrazioni un'ulteriore sforzo nell'arduo compito di intendere la protezione dei dati quale strumento utile a garantire trasparenza nel rapporto tra Amministrazione dello Stato e cittadino[2].

Il Regolamento UE 2016/679 fotografa, ai considerando 6 e 7, una delle caratteristiche salienti della nostra società: la rapidità dell'evoluzione tecnologica che comporta una produzione e un'analisi dei dati personali come mai in precedenza. Le nuove tecnologie offrono enormi opportunità alla collettività in tutti i settori dall'attività di impresa, ai servizi resi dalla pubblica amministrazione e alla ricerca scientifica.

La crescita esponenziale dei dati, oggetto di trattamento, comporta inevitabilmente anche un enorme aumento dei rischi per i diritti e le libertà fondamentali degli interessati che occorre bilanciare attraverso l'adozione di idonee contromisure.

Come noto, anche la pubblica amministrazione non è estranea a questo scenario. Le banche dati pubbliche, infatti, rappresentano, per estensione e profondità, uno dei giacimenti più rilevanti dei dati inerenti all'intera popolazione italiana e l'applicazione di tecniche avanzate di analisi (data mining, big data, intelligenza artificiale), anche in questo contesto, costituiscono uno dei temi più sfidanti dell'applicazione della disciplina di protezione dati contemporanea.

Gli elementi di approfondimento e le criticità sono diversi e attengono: alla individuazione della corretta base giuridica del trattamento e alle sue caratteristiche, soprattutto in relazione all'uso di sistemi sofisticati di profilazione su larga scala o all'utilizzo di sistemi parzialmente o esclusivamente automatizzati per l'assunzione di decisioni (algoritmi); alla verifica della sussistenza dei requisiti richiesti dalla legge per procedere a scambi dati tra le pubbliche amministrazioni, ivi comprese la definizione di corrette misure di sicurezza volte a garantire l'integrità e la riservatezza dei dati; alla corretta gestione di procedure di accesso alle banche

[1] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali,* I diritti nella "rete" della rete, Giappichelli Editore, p. 48.

[2] G.M. PELLOS, *Manuale di diritto alla protezione dei dati personali,* Maggioli Editore, p. 601.

dati pubbliche da parte di decine di migliaia di utenti abilitati, prevedendo la tracciabilità degli accessi, nonché idonei sistemi di *alert* volti a segnalare, in via preventiva, probabili comportamenti anomali sintomatici di possibili abusi.
Sulla scorta di quanto sin qui rappresentato, gli Enti pubblici dovranno implementare azioni volte al rispetto del principio di *Privacy by Design*, sin dalla fase di progettazione, e di *Privacy By Default*, prevedendo un idoneo apparato organizzativo al fine di ridurre al minimo possibili violazioni alla disciplina rilevante in ambito privacy.
Il presente lavoro offre spunti di riflessione per gestire i flussi di dati personali nel settore pubblico in conformità ai principi e alla normativa rilevante in materia di protezione dei dati personali. L'adozione di modelli Organizzativi di Gestione e controllo della Privacy, adeguatamente strutturati, permetterà, in qualsiasi contesto, di affrontare e superare le problematiche correlate a violazione dei dati o attività di tipo ispettivo condotte dall'Autorità Garante, mitigando i rischi di tipo operativo, reputazionale, economico e sanzionatorio. E' importante che le pubbliche amministrazioni siano responsabili (in applicazione del principio di accountability, espressamente previsto dall'art. 24 del Regolamento UE 2016/679) della conformità alle regole di protezione dati dei trattamenti effettuati, e finanche gli interessati stessi, siano cauti nell'utilizzo delle nuove potenzialità offerte dalla rete e dai nuovi strumenti tecnologici.

2. La comunicazione delle banche dati tra pubbliche amministrazioni e i rischi legati alla protezione dei dati personali

L'abrogato art. 58 del CAD prevedeva, in un'ottica di fruibilità delle informazioni, la possibilità, per le pubbliche amministrazioni, di stipulare apposite convenzioni per la consultazione e la comunicazione di dati personali utili all'assolvimento delle funzioni istituzionali. La lenta ma costante evoluzione degli Enti pubblici richiede operazioni di scambio di dati con altre amministrazioni sempre più frequenti, ragione per cui è necessario definire le finalità[3] per le quali si rende necessaria la consultazione di determinate informazioni appartenenti ai cittadini, onde evitarne un uso improprio degli stessi.
La comunicazione dei dati personali per l'esecuzione di un interesse pubblico o connesso all'esercizio dei pubblici poteri, ad oggi è disciplinato dall'art. 2-*ter*, del Codice in materia di protezione dei dati personali, lì dove è previsto che la base giuridica debba essere rappresentata da una disposizione di legge, o nei casi previsti dalla legge, di regolamento o, in mancanza, dallo svolgimento di compiti di interesse pubblico e delle finalità istituzionali previa comunicazione al Garante[4].
Sempre all'interno dello stesso articolo del Codice, al comma 4, il legislatore italiano, opportunamente, ribadisce la differenza sostanziale tra comunicazione e diffusione[5] di dati personali, riferendo, per la prima fattispecie, *"il dare conoscenza dei dati personali a uno o più*

[3] F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, Lulu Editore, 2015, p. 132*
[4] D.Lgs 30 giugno 2003, n.196 integrato con le modifiche dal D.Lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679", versione rinvenibile sul sito del Garante per la protezione dei dati personali (www.garanteprivacy.it).
[5] F. MODAFFERI nel ciclo di eventi formativi organizzati dall'Autorità Garante per la protezione dei dati personali alla luce dell'entrata in vigore del Regolamento generale UE 2016/679, (https://www.garanteprivacy.it/regolamentoue/formazione/).

soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento di dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione", mentre per la seconda *"il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"*. E' questa, una distinzione lineare sotto il profilo concettuale, ma che ha portato negli anni scorsi e tutt'ora, alcuni Enti pubblici ad essere oggetto di richiamo da parte del Garante per la protezione dei dati personali. Si pensi, a titolo esemplificativo, alle sanzioni irrogate dall'Autorità italiana a garanzia della riservatezza per le pubblicazioni di dati identificativi all'interno di graduatorie di percettori di sussidi economici da parte dei Comuni o per la diffusione sul sito istituzionale dell'Ente pubblico di informazioni di natura particolare (non più sensibili, ai sensi dell'art. 9, paragrafo 1 del Regolamento UE 2016/679) riferite a persone disagiate sotto il profilo psico-fisico, economico e sociale[6]. Emblematico è, in ordine di tempo, il caso del Comune di Messina che è stato inibito dal Garante per la protezione dei dati personali a pubblicare, in chiaro, le informazioni di natura personale di 3447 cittadini che avevano usufruito di esenzioni o riduzioni sulla tassa dei rifiuti riferita all'anno 2015[7]. Definita la differenza tra comunicazione e diffusione nella normativa privacy, è necessario procedere all'analisi di ulteriori criticità nello scambio di informazioni.

Con riferimento all'acquisizione di "nuovi" dati, le pubbliche amministrazioni dovrebbero valutare e verificare se le informazioni di cui necessitano possano essere reperibili tramite accesso e consultazione di banche dati di altri soggetti pubblici. Tale scambio viene espressamente previsto dal Capo V, *Disponibilità dei dati delle pubbliche amministrazioni*, del Codice della amministrazione digitale, lì dove all'art. 50, comma 1, dispone che "*i dati della pubblica amministrazione sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione alle condizioni fissate dall'ordinamento*". Il contesto operativo è rappresentato dal Sistema Pubblico di Connettività[8], l'infrastruttura che rende possibile il coordinamento informativo e informatico dei dati tra amministrazioni pubbliche, centrali e locali, al fine di garantire, in maniera conforme, la trasmissione dei dati tra Enti pubblici: lo scambio di documenti informatici secondo il Sistema, nel pieno rispetto delle misure procedurali e di sicurezza, equivale ad invio documentale valido ad ogni effetto di legge.[9]

Sempre l'art. 50 del Codice dell'amministrazione digitale, all'art. 2 prevede espressamente che qualsiasi dato trattato dalla pubblica amministrazione debba essere reso accessibile e fruibile ad altra amministrazione, richiamando, per certi versi, l'abrogato art. 58 del Codice. È facilmente intuibile, quindi, che a fronte della indiscussa utilità di poter consultare

---

[6] Garante per la protezione dei dati personali, *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*, 2014.

[7] Provvedimento del Garante per la protezione dei dati personali rinvenibile sul sito www.garanteprivacy.it, doc. web n. 8576011.

[8] Si veda al riguardo DPCM 1 aprile 2008, *Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività.*

[9] Art. 76 del Codice dell'amministrazione digitale.

informazioni e dati tra pubbliche amministrazioni[10] con lo scopo di verificare, ad esempio, la veridicità delle dichiarazioni sostitutive riguardanti dati relativi a stati, qualità personali e fatti di cui agli artt. 46 e 47 del D.P.R. 28 Dicembre 2000, n.445, si evidenzia una forte criticità rispetto al diritto all'identità personale, alla riservatezza e alla protezione dei dati personali dei cittadini alla luce del Regolamento UE 2016/679 che, tra le finalità dichiarate, pone la salvaguardia dei diritti e le libertà fondamentali delle persone fisiche.
La pubblica amministrazione, al pari di ogni altro titolare del trattamento, è tenuta ad adottare misure logiche di sicurezza[11] finalizzate alla protezione dei sistemi informatici e, di conseguenza, all'integrità del dato per dimostrare un atteggiamento *accountable* nei confronti delle disposizioni del legislatore europeo in materia di protezione dei dati personali[12].
Uno studio svolto sui principali siti web italiani, ha evidenziato che circa il 40% di questi utilizza ancora connessioni non sicure nello scambio di dati e che oltre l'80% non fornisce i recapiti per l'esercizio dei diritti dell'interessato o i dati di contatto del Data protection officer e questo penalizza non solo le libertà fondamentali delle persone fisiche ma anche le stesse aziende che, a questo modo, sprecano molte delle opportunità del mercato digitale13. L'obiettivo dichiarato dell'UE, con l'introduzione del GDPR, è quello di creare un clima di fiducia per lo sviluppo dell'economia digitale in tutto il mercato interno. Quando le aziende italiane comprenderanno il valore dei dati personali, si potrà innescare un meccanismo virtuoso, indispensabile per lo sviluppo del proprio business e, la conformità al GDPR sarà considerata, non solo mero obbligo, ma un investimento.
Il Garante per la protezione dei dati personali, alla luce del mutato scenario normativo, svolge un ruolo determinante per le tematiche aventi ad oggetto lo scambio di dati personali nella pubblica amministrazione, lì dove ha contribuito, nel recente passato, alla pubblicazione in Gazzetta Ufficiale, n. 179 del 4 agosto 2015, di un Provvedimento di cui si esamineranno gli aspetti salienti. Durante questo intervento, l'Autorità ha posto l'accento sugli impatti rilevanti sotto il profilo della tutela della riservatezza, dell'identità personale e della protezione dei dati personali, rilevando il valore e la responsabilità delle parti coinvolte quali erogatori, intesi quali soggetti che garantiscono la disponibilità, anche tramite stipula di convenzione o altro atto giuridico bilaterale, strumento che l'attuale CAD consente di superare e che l'art. 15 della L. 241/1990 contempla[14], delle banche dati ai fruitori.

3. Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche

L'Autorità Garante per la protezione dei dati personali, per i profili di competenza, ha posto particolare attenzione allo scambio di dati personali tra pubbliche amministrazioni ha

[10] Agenzia per l'Italia Digitale, *Linee guida per la stesura di convezioni per la fruibilità di dati delle pubbliche amministrazioni*, 2013.
[11] Circolare n. 2/2017 AGID, *Misure minime di sicurezza ICT per le pubbliche amministrazioni*.
[12] *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*, www.garanteprivacy.it.
[13] Studio svolto dall'Osservatorio *Federprivacy* sui principali trecento siti web italiani alla vigilia della piena entrata in vigore del Regolamento UE 2016/679 il 25 maggio 2018.
[14] L. CAPICOTTO, *Commento alla sentenza della corte di giustizia Ue – grande sezione – 19 dicembre 2012. Elementi identificativi degli accordi di cooperazione, ex art. 15 legge 241 del 1990 e s.m.i. e obbligo di rispettare le regole dell'unione europea sugli appalti pubblici*, Gazzetta Amministrativa, Numero 4/2012.

emanato un intervento di natura dispositiva in data 2 luglio 2015[15]. Tale provvedimento continua a produrre effetti nelle parti compatibili con il Regolamento UE 2016/679, auspicando che la stessa Autorità, così come disposto nell'art. 2-*quinquiesdecies* del D.Lgs n.101/2018, possa intervenire con propri provvedimenti, qualora i trattamenti necessari per l'esecuzione di un compito di interesse pubblico, presentino un rischio elevato per i diritti e le libertà delle persone fisiche, lì dove si verrebbe a configurarsi, altresì, la necessità di effettuare la valutazione di impatto privacy, tenendo conto, in ultimo, delle indicazione del Garante[16].

Preme ricordare che il suddetto provvedimento elenca una serie di misure rilevanti sotto il profilo della tutela dei dati personali tenendo dovutamente conto delle disposizioni e degli obiettivi contenuti nel Codice per l'amministrazione digitale. Con riferimento alle modalità di accesso alle diverse tipologie di dati tra pubbliche amministrazioni, molteplici sono le opzioni tecniche, come l'accesso via web attraverso sito istituzionale dell'Ente erogatore o tramite applicazioni software, la consultazione tramite la cooperazione applicativa sfruttando il sistema pubblico di connettività, l'accesso attraverso la posta elettronica certificata nel caso in cui tale modalità, data l'occasionalità e la portata limitata dello scambio di informazioni, presenti vantaggi economici per le amministrazioni coinvolte o la consultazione attraverso soluzioni di "Trasferimento file" in modalità *File Transfer Protocol*[17] sicuro con la cifratura del canale di trasmissione dei dati.

Come riferito in precedenza, lo strumento attraverso il quale legittimare lo scambio di informazioni tra pubbliche amministrazioni può essere rappresentato dalla convenzione (o qualsiasi altro atto bilaterale tra erogatore e fruitore), con la quale vengono specificate, in maniera tassativa, le misure di sicurezza dei sistemi informativi, la gestione dei profili di autorizzazione, al fine di tracciare e verificare gli accessi da parte di personale autorizzato alla consultazione dei dati scongiurando, così, la possibilità di accessi non consentiti e, in ultimo le garanzie sotto il profilo della riservatezza, in piena adesione alla normativa nazionale ed europea in materia di protezione dati personali.

Nel provvedimento, forte è il riferimento al "vecchio" responsabile del trattamento e all'incaricato del trattamento, figure incardinate ai sensi degli artt. 29 e 30 del "vecchio" Codice in materia di protezione dei dati personali[18]. Il nuovo quadro normativo europeo e italiano (con l'intervento del settembre 2018) non prevedono un espresso obbligo di designazione in capo al titolare del trattamento di tali figure, rimandando, per questa fattispecie, ancora al principio di accoutability: la *compliance* della pubblica amministrazione richiede, tra le altre attività da porre in essere, l'attribuzione di compiti e responsabilità al personale interno dell'Ente pubblico.

A sostegno di quanto sin qui affermato, il Regolamento UE 2016/679 non prevede espressamente queste figure, se non attraverso l'analisi di alcuni articoli. L'art. 28, durante i primi mesi di applicazione della normativa europea privacy, era stato oggetto di diverse interpretazioni secondo le quali il responsabile del trattamento potesse essere ancora

[15] Provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015, www.garanteprivacy.it

[16] Si veda a tal riguardo anche il contributo del Gruppo Articolo 29, *Linee guida in materia di valutazione di impatto sulla protezione dei dati (WP248).*

[17] V. CAPUANO, G.I. Gargiulo, *Il Protocollo FTP,* Creative Commons, 2008, p. 6.

[18] F. MODAFFERI, *Lezioni di diritto alla protezione dei dati personali, cit.* pp. 198-200.

"interno". Tale diversità di vedute è stata risolta a seguito di più attento studio della normativa europea in materia di protezione dei dati personali e delle indicazioni diramate dall'Autorità nelle attività formative per le pubbliche amministrazioni. Resta salva, per il titolare, la possibilità di prevedere, così come previsto dall'art. 2-quaterdecies, che nell'ambito del proprio assetto organizzativo specifiche funzioni siano attribuite a persone designate. Il Regolamento UE 2016/679, inoltre, non fa più espresso riferimento alla figura dell'incaricato, ma prevede agli artt. 4, n. 10), 29, e 32 che determinate operazioni di trattamento sui dati personali vengano effettuate da persone istruite in tal senso dal titolare. In un contesto nel quale è forte l'auspicio per una collaborazione sinergica nello scambio dati tra pubbliche amministrazioni, strategico è il ruolo giocato da figure espressamente previste dal legislatore italiano ed europeo: il Responsabile della transizione digitale, passando per l'Amministratore di sistema[19], il Responsabile del sistema di conservazione dei documenti informatici e il Responsabile della protezione dei dati personali. Proprio l'art. 44, commi 1-*bis* e 1-*ter* del CAD pone l'accento (anche lì dove si parla di responsabile del trattamento secondo la vecchia e abrogata formulazione dell'art. 29 del D.Lgs n,196/2003) sulla necessità, per le pubbliche amministrazioni, di garantire autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici in un'ottica di *business continuity*[20].

Nel provvedimento dell'Autorità sulle "misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche", il Garante prevede che, in una fase preliminare alla stipula della convenzione, il soggetto erogatore debba verificare la base normativa e le finalità istituzionali[21] che legittimano il soggetto fruitore all'accesso e controllare, in base alla infrastruttura tecnologica, alla quantità dei dati richiesti e il numero del personale autorizzato alla consultazione, la modalità telematica adeguata per garantire l'accesso al soggetto fruitore. Tale provvedimento prevede un serie di compiti in capo al soggetto erogatore, il quale, in qualità di titolare del trattamento, deve rispondere ad uno degli attuali principi ispiratori del Regolamento generale sulla protezione dei dati personali UE 2016/679: la responsabilizzazione. Agli attori protagonisti delle attività di interesse pubblico è richiesto il rispetto del principio di finalità del trattamento, per cui le pubbliche amministrazioni, nella fase immediatamente successiva della *Privacy by design*, possono trattare solo dati necessari al solo perseguimento delle finalità da raggiungere. Così come altri obblighi imposti dal legislatore europeo in materia di protezione dei dati personali, la *Privacy by default* impone al titolare del trattamento misure proattive, dinamiche e finalizzate ad attenuare il rischio per i diritti degli interessati[22]. Accanto al principio di finalità del trattamento, oggi richiamato dall'art. 5, lett. b) del Regolamento UE 2016/679, l'Autorità, nel provvedimento oggetto di studio, richiama l'importanza, per le pubbliche amministrazioni, di prevedere adeguati e precisi profili di autorizzazione dei soggetti incaricati, onde evitare casi di accessi non

[19] Provvedimento del Garante per la protezione dei dati personali Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).

[20] C. RANDIERI, *Ingegneria della Business Continuity: una nuova opportunità*, Wolters Kluwer, Ingegneri.info, 31 maggio 2018.

[21] Nonostante l'art. 58 CAD sia stato abrogato, si vedano le *Linee guida per la stesura di convenzioni per la fruibilità di dati personali delle pubbliche amministrazioni.*

[22] F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali,* II, Giappichelli Editore, 2016, p. 43.

autorizzati. Occorre, pertanto, individuare una figura con alcune competenze specifiche ed altre trasversali, in grado di scongiurare o, comunque, ridurre al minimo i rischi di violazione dati che posano esporre a sanzioni civili e penali, e anche per prevenire l'insorgere di contenziosi legati a scarsa trasparenza nell'utilizzo di dati personali all'interno dell'organizzazione pubblica.

La protezione dei dati personali si sposta sempre più sul *web* e il grosso dell'azione è rivolta, oramai, alle nuove tecnologie che hanno cambiato il modo di vivere ed in particolare il lavoro e il mercato. Siamo di fronte ad una realtà tutta nuova, in cui il compito del responsabile della protezione dei dati personali è garantire, tra gli altri, equilibrio tra gestione e salvaguardia della *privacy*[23]. Sono perciò richieste competenze digitali per gestire gli impatti della rivoluzione tecnologica sul diritto della protezione dei dati personali e l'attività di chi deve garantire controllo e uso corretto, deve necessariamente digitalizzarsi. Il Regolamento UE 2016/679 ha compiuto grandi passi in avanti in questo senso, ma per poter completare il nuovo *frame work* di protezione europeo occorre seguire regole sempre più chiare, più forti e più intelligenti per la tutela in rete.

[23] Si veda *Big data e privacy*, Atti del convegno del 30 gennaio 2017, intervento del Presidente Soro.