I MECCANISMI DI CERTIFICAZIONE DELLA TUTELA DEI DATI PERSONALI, TRA GDPR E NORMATIVA INTERNA

ERMANNO SALERNO*

Sommario

Suggerimento di citazione

E. SALERNO, *I meccanismi di certificazione della tutela dei dati personali, tra GDPR e normativa interna*, in *Osservatorio sulle fonti*, n. 1/2019. Disponibile in: http://www.osservatoriosullefonti.it

*Dottore in Giurisprudenza, Cultore della materia di Diritto Costituzionale presso l'Università degli Studi di Firenze.

Contatto: ermanno.salerno@unifi.it

Registrazione presso il Tribunale di Firenze n. 5626 del 24 dicembre 2007
Rivista inclusa nella classe A delle Riviste scientifiche di Area 12 – Direttore Prof. Paolo Caretti
ISSN 2038-5633

1. Introduzione

Nel dicembre 2015 il Parlamento Europeo, la Commissione e il Consiglio hanno raggiunto un accordo per una serie di riforme alla normativa riguardante la protezione dei dati personali. Il Regolamento UE 679/2016, ovvero il *General Data Protection Regulation* (da qui, GDPR), è entrato in vigore il 24 maggio 2016, ma vi è stata data applicazione soltanto a partire dal 25 maggio 2018 (in base all'art. 99.2 del GDPR stesso). Il D.lgs. 101/2018, entrato in vigore dal 19 settembre 2018, ha apportato consistenti modifiche al D.lgs. 196/2003 (c.d. Codice della Privacy). In questo quadro di riforma complessiva della disciplina europea e interna, il contributo si focalizza sui meccanismi di Certificazione (del rispetto della disciplina a tutela dei dati personali); un istituto che difficilmente può essere accostato alle categorie del nostro diritto positivo, poiché, per le ragioni di seguito evidenziate, si pone al confine tra un atto privatistico e una fonte normativa. Ecco perché merita quantomeno tentare un inquadramento giuridico della Certificazione.

2. Il quadro normativo europeo precedente in materia di privacy

Partendo dall'assunto che il D.lgs. 101/2018 non fa altro che recare "disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento [GDPR, *ndr*]", merita procedere alla disamina del quadro normativo europeo in materia di *privacy*, in seguito alle riforme recenti[1].

Il GDPR sostituisce la precedente disciplina europea in materia di protezione dei dati personali, contenuta nella Direttiva 95/46/CE (Giovannella, 2017). Questa è stata recepita in Italia prima con la L. 675/1996 e poi con il D.lgs. 196/2003 (una sorta di T.U. in materia di trattamento dei dati personali, il cd. Codice della Privacy), come noto; tuttavia, il recepimento italiano ha frainteso in parte l'oggetto della tutela. Infatti, come ricorda certa dottrina (Beccara, 2018), esiste un rapporto di *genus* a *species* tra *privacy* e "protezione dei dati personali": la prima rappresenta un insieme più ampio, in grado di ricomprendere *anche* il diritto alla seconda (per questo, all'art. 2 del vecchio Codice si identificava la *privacy* come sommatoria di tre distinti diritti, ossia il *diritto alla riservatezza*, il *diritto all'identità personale* e, per l'appunto, il *diritto alla protezione dei dati personali*)[2].

[1] Così il nuovo art. 2 del D.lgs. 196/2003, come modificato dal D.lgs. 101/2018. Nel nuovo art. 1 del Codice Privacy si specifica che "Il trattamento dei dati personali avviene secondo le norme del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016…e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona". Si veda, per esempio la raccolta di contributi su *Il Civilista*, *Speciale Riforma*, L. BOLOGNINI e E. PELINO (a cura di), *Codice Privacy: tutte le novità del d.lgs. 101/2018*, Giuffré Francis Lefebvre, 2018.

[2] J.L. BECCARA, *La privacy nel pubblico: sintesi dell'integrazione tra Codice italiano e Regolamento europeo per la Pubblica Amministrazione*, FrancoAngeli, Milano, 2018, 17.

Il contributo, per quanto sia possibile, mira proprio ad analizzare un istituto del *genus* GDPR (i meccanismi di Certificazione) per provare a fornire un'ipotesi di inquadramento normativo a livello di *species*.

2.1. La precedente tutela europea dei dati personali

La Direttiva 95/46/CE aveva alcune lacune, come di seguito evidenziate, che hanno portato il legislatore europeo a sostituirla col GDPR. Per quel che si rende necessario per affrontare il tema del contributo, due sono in particolare le lacune che contano.

Innanzitutto, nella Direttiva 95/46/CE non si faceva affatto riferimento allo strumento della Certificazione per l'attestazione del rispetto della tutela dei dati personali; da questo punto di vista, si può affermare che il GDPR abbia introdotto una forte novità.

In secondo luogo, la prospettiva della (vecchia) Direttiva era caratterizzata da una c.d. *verticalità*. Tale atto normativo, proprio per sua natura giuridica, imponeva degli obblighi minimi di tutela dei *metadati* (e dei dati personali in generale), ma, come noto, demandava agli Stati Membri la definizione in concreto delle sanzioni nei confronti di coloro che si fossero resi responsabili di violazioni degli obblighi stessi[3].

In sintesi, due erano le caratteristiche della precedente normativa europea, oggetto poi della riforma recente: la verticalità della disciplina e l'assenza dello strumento certificatorio[4]. Ovviamente, entrambe portavano con sé dei problemi.

Riguardo alla prima, la normativa (europea e, *a fortiori*, interna) si è dimostrata nel tempo inefficace, oltre che inadeguata allo sviluppo delle tecnologie (*social networks*, intelligenze artificiali, flusso di dati in internet o da satellite)[5]; oltretutto, essa aveva un'efficacia territoriale limitata al *territorio* CE/UE (*ex* art. 10), di tal che il cittadino europeo poteva essere protetto soltanto entro i confini di essa, ma non al di fuori (su cui interviene il GDPR, come Regolamento)[6].

[3] Si vedano gli artt. 24 e 25 della Direttiva 95/46/CE: il primo demanda agli Stati Membri un'adeguata *sanction policy*; il secondo impone che il Paese (soltanto CE/UE, non extracomunitario), nel quale il dato personale viene trasferito, assicuri un adeguato livello di protezione.

[4] Si veda E. LACHAUD, 2018, cit.

[5] Uno dei motivi principali è la totale mancanza, in capo alle Autorità Garanti nazionali, di possibilità gestionale ed economica utile a intervenire, *in primis*, e risolvere, *in secundis*, l'eventuale violazione delle norme sul trattamento dei dati personali (a livello interno, europeo o internazionale). Spesso, per mancanza di tempo, risorse e competenza, esse riescono ad agire su un numero molto ristretto di casi. Ma bisogna anche ricordare che la Direttiva in questione nacque in un tempo in cui internet era ancora agli albori e i cellulari avevano ancora vistose antenne e batterie. Si veda sul punto J.L. BECCARA, cit.,13-15.

[6] La precedente Direttiva aveva perciò delle evidenti lacune anche da questo punto di vista, soprattutto di fronte allo sviluppo della globalizzazione. Si veda la giurisprudenza della CGUE in

Riguardo alla seconda, si potrebbe affermare che il controllo sull'effettiva tutela dei dati personali dei cittadini europei sia stato affidato agli Stati Membri, i quali, nel tempo, hanno singolarmente prodotto proprie normative (quindi eterogenee). Ma senza uno strumento certificatorio adeguato ed unitario in tutto lo spazio giuridico europeo, tutto il meccanismo tendeva a gravare sulle Autorità Garanti nazionali, incaricate di controllare potenzialmente tutti ma poi, in concreto, *pochi* responsabili (e/o incaricati) del trattamento dei dati personali[7].

3. La disciplina del GDPR

La differenza del GDPR con la normativa precedente si coglie già con la lettura del *Considerando n. 9*, a mente del quale il legislatore eurounitario riconosce espressamente che la Direttiva 95/46/CE "non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione…che…le operazioni *online* comportino rischi per la protezione delle persone fisiche"[8]. In altre parole, come già anticipato, il GDPR in quanto Regolamento dell'Unione Europea, ha l'indubbio vantaggio (rispetto alla precedente normativa comunitaria) di dover essere applicato uniformemente in tutti gli Stati Membri. Inoltre, onde superare i ristretti limiti territoriali che possedeva la Direttiva 95/46/CE, esso verrà applicato in generale a tutti i cittadini dell'UE, ovunque essi siano, qualora vengano trattati i loro dati personali[9].

L'elemento fondamentale per l'applicazione del GDPR è l'*attività* del trattamento dei dati personali: se essa viene svolta all'interno dell'UE o su cittadini UE, dovrà rispettare la normativa del GDPR, che ci si riferisca a un *trattamento automatizzato* (p.e. da parte dei gestori delle pagine web), ovvero a un *trattamento non automatizzato* (p.e. da parte di un datore di lavoro nei confronti di un lavoratore)[10]. In altre parole, il Regolamento si applica ai

Google Spain SL, *Google Inc. v Agencia Española de Proteccion de Datos*, *Mario Costeja Gonzalez*, Case C-131/12.

[7] Si veda J.L. BECCARA, cit., 32, secondo il quale nella precedente normativa v'era una *discrasia* tra le figure giuridiche del *Responsabile* del trattamento dei dati personali e l'*Incaricato* (ma che si invertivano a livello comunitario in quanto a definizioni). Il GDPR e, di conseguenza, il Codice Privacy italiano, come modificato nel 2018, hanno ovviato a tale discrasia.

[8] Si veda, a tal proposito, E. LUCCHINI GUASTALLA, *Il nuovo Regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e Impresa*, 2018, 1, 106.

[9] Si veda l'art. 3 GDPR, per il quale il Regolamento si applica se il responsabile o gestore dei dati personali ha la propria sede (o la propria attività) nel territorio dell'Unione, oppure se i dati personali trattati appartengono ad un cittadino dell'Unione, ovunque egli si trovi. Nel Codice, modificato dal D.lgs. 101/2018, non si fa riferimento al principio di territorialità (salvo che non si tenti una forzatura, argomentando sull'art. 27 del Codice).

[10] E. LUCCHINI GUASTALLA, cit., 106 ss.

Titolari (coloro che possiedono un dato personale, cioè i cittadini UE), così come ai *Responsabili* (coloro che tratteranno il dato personale, anche attraverso Incaricati, di cui *infra*) che hanno uno *stabilimento in UE* ed effettuano il trattamento, di qualunque genere esso sia, nel contesto delle attività dello *stabilimento* stesso (a prescindere da dove il trattamento sia concretamente effettuato), nonché a *Titolari* e *Responsabili* che, pur non avendo uno stabilimento in UE, effettuino il trattamento dei dati di soggetti che si trovino in UE (criterio di collegamento fisico, o anche solo virtuale), per l'offerta di beni o servizi (gratuita o meno), ovvero per effettuare un monitoraggio[11].

A maggior riprova di quanto appena detto, lo scopo materiale del Regolamento, come espresso dall'art. 2 GDPR, è di disciplinare qualsiasi tipo di trattamento (*processing*) del dato personale, nel senso più onnicomprensivo possibile (a tal proposito, il nostro Codice Privacy dedica i principi *ex* artt. 2-*ter* e ss., nonché le norme speciali per settori differenti nei Titoli II e ss.)[12].

Trattare un dato personale è un *procedimento*, costituito da una o più operazioni realizzate *sul* dato personale, ovvero su una *pluralità* di essi, con o senza automatismi (*automated means*)[13]. Naturalmente, si fa riferimento a trattamenti sia *manuali*, eseguiti cioè da persone (*humans*, secondo la definizione di Voigt), senza l'impiego di macchine, così come *automatizzati*, posti in essere cioè da intelligenze artificiali o con l'impiego di strumenti informatici [14].

[11] Così, J.L. BECCARA, cit., 42, in relazione al Considerando n. 24 del Regolamento.

[12] C'è da dire che la tutela del dato *non-personale* venga dal GDPR tralasciata. Su questo dovranno intervenire le normative speciali europee, oppure quelle interne degli Stati Membri. Manca nel D.lgs. 101 una disciplina al riguardo, per ovvie ragioni. Si veda, per il commento sulla normativa europea, VOIGT, cit.; per il commento sulla normativa interna, L. BOLOGNINI, E. PELINO, cit., 17 ss.

[13] Si veda l'art. 4, n. 2) del GDPR, il quale elenca una lunga lista di operazioni (non esaustiva) che rappresentano ipotesi esemplificative di trattamento di dati personali automatizzati o meno: "«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". Al riguardo, il D.lgs. 101 dedica gli artt. 2 e ss. alla disciplina del trattamento, con svariate normative speciali nei Titoli I-XII dedicate alle categorie particolari di dati personali.

[14] L'art. 2.1 GDPR disciplina in modo attento l'impiego del trattamento "manuale", seppur in modo ondivago: i requisiti e gli obblighi che devono essere rispettati per non violare la normativa europea nuova appaiono puntigliosi e quasi senza una logica ben precisa. Infatti, la norma in questione richiede che il dato venga inserito all'interno di un *filing system* (un raggruppamento di dati accessibile secondo precisi criteri, centralizzato o delocalizzato), preconfezionato come modello standard (*Considerando* n. 15), e strutturato, secondo specifici criteri, in differenti gruppi o categorie per la sua gestione integrata e condivisa con gli altri.

Peraltro, come sopra accennato, il dato personale[15] può rilevare sia a livello informatico che a livello materiale ed è definito in dottrina, in senso stretto, come *qualsiasi tipo di informazione raccolta*, *segni* o *indicazioni*, che riguardi un *identificato o identificabile individuo*[16]. In senso lato, è definibile dato personale anche tutto ciò che, attraverso incroci di informazioni disponibili, permetta di identificare un determinato cittadino UE (p.e. le sue *caratteristiche* fisiche, economiche, sociali, genetiche, culturali, ecc.)[17]. L'unico limite a quest'ampia definizione di dato personale è la morte di una persona: il Regolamento non può essere applicato ai dati personali di una persona deceduta, sulla scorta del *Considerando* n. 27 GDPR; così da permettere, per esempio, ad un parente o a chi abbia interesse di conoscere informazioni (anche "sensibili") del defunto, come malattie genetiche o movimenti bancari pregressi, per un interesse giuridicamente rilevante[18].

Il GDPR viene applicato, inoltre, a tutti coloro che trattano o che controllano il trattamento dei dati personali (entrambi soggetti che, nel nostro Codice Privacy, come modificato dal D.lgs. 101/2018, vengono identificati nelle figure di *Responsabile* e *Incaricato*)[19]. È bene ricordare che il Responsabile opera sempre sulla scorta di una capacità propria direzionale e di un certo grado di determinazione in merito agli strumenti del trattamento[20]; proprio per questo ha degli obblighi molto stringenti (da quelli più generici

[15] Art. 4, n. 1) del GDPR: "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

[16] P. VOIGT, cit., 11.

[17] Per incroci di informazioni si può fare l'esempio di una normale navigazione in internet (alla quale si riferisce *de relato* il Considerando n. 24 del Regolamento): il nome di una persona, il suo numero identificativo, il suo ID, il suo VPN di connessione, i dati IP o di navigazione, sono tutte "tracce" che permettono la comprensione delle caratteristiche soggettive di un individuo da parte di coloro che gestiscono siti internet (visitati), motori di ricerca o *social networks*. È evidente quanto fosse obsoleta la vecchia disciplina della Direttiva 95/46/CE; ed è ancor più evidente quanto già lo stesso Regolamento sia soggetto a rapido invecchiamento.

[18] Eventualmente starà alle normative nazionali stabilire dei ragionevoli controlimiti. Sul punto si veda il contributo di E. PELINO, in L. BOLOGNINI, E. PELINO, cit., 73-76.

[19] Si vedano le definizioni di "controller" e "processor" contenute nell'art. 4, nn. 7-8 del GDPR. Tuttavia la loro distinzione è meramente formale; per questo le due figure possono essere trattate congiuntamente. Sul punto, rispetto alla normativa interna modificata nel 2018, si veda J.L. BECCARA, cit., 76 ss.

[20] Elementi che lo distinguono dall'Incaricato (ex art. 30 del Codice e artt. 29 e 32.4 del Regolamento), come indica J.L. BECCARA, cit., 81, il quale è un soggetto subordinato del Responsabile e chiamato a gestire il dato personale in nome e per conto del Responsabile.

sull'informativa al Titolare, fino a quelli specifici e rigorosi sul trattamento dei dati biometrici o genetici)[21].

Tuttavia, merita precisare, la *forma giuridica* del Responsabile o dell'Incaricato del trattamento dei dati personali non è rilevante per il corretto adempimento degli obblighi presenti nel GDPR; infatti, che esso sia un ente pubblico o privato, un comune italiano o una S.p.A., non fa differenza. Se un soggetto può essere identificato come Responsabile o Incaricato del trattamento di dati personali, proprio perché chiamato a gestirli, dovrà rispettare le regole del GDPR.

C'è un ulteriore aspetto da evidenziare: l'introduzione da parte del GPDR di una figura manageriale in ordine alla tutela dei dati personali operata da Responsabili e Incaricati. Nella realtà quotidiana, infatti, il Responsabile o l'Incaricato dovranno avvalersi di persone in carne ed ossa per la gestione in concreto dei dati personali loro affidati dai Titolari; per questo motivo è stata introdotta (artt. 37-39 del Regolamento) una nuova figura, il cd. *Data protection officer*. Un soggetto esperto della normativa e prassi (nazionale ed europea) del trattamento dei dati personali, interfaccia e punto di collegamento tra l'ente, pubblico o privato, di cui fa parte, e l'Autorità Garante per la Privacy (nazionale), che concorre alla gestione dei dati personali (di cui l'ente è Responsabile) e alla produzione del c.d. *Data Protection Impact Assessment*[22]. Tuttavia è una figura obbligatoria se l'ente privato (come un'azienda, per esempio) supera la soglia dei 25 dipendenti e se il trattamento dei dati personali è parte integrante del suo *core business*. Altrimenti, il DPO resta meramente facoltativo, benché consigliabile[23].

Ulteriori novità introdotte dal Regolamento sono le diversificazioni del concetto di "dato personale", come "dato biometrico" o "dato di salute" o "dato genetico", contenute nell'art. 4; oppure, le diverse definizioni di *privacy*

[21] C'è da dire che a livello interno, le modifiche introdotte al Codice Privacy dal D.lgs. 101/2018 siano state, se possibile, ancor più rigorose e puntigliose della normativa eurounitaria (v. *supra*, le diverse categorie di trattamento dei dati personali).

[22] Come risulta dal combinato disposto degli artt. 7, 35 e 37 GDPR. Si veda anche P. VOIGT, cit., 50; F. GIOVANNELLA, cit., 180; J.L. BECCARA, cit., 82.

[23] Per le società private essa rappresenta sicuramente un elemento di *management* importante sotto il profilo della gestione dei dati personali. Tuttavia, avendo un costo nel bilancio delle stesse, spesso e volentieri viene scelto un dipendente interno dell'azienda (e non un consulente esterno, il c.d. *privacy manager*), purché possegga competenze adeguate, per ricoprire efficacemente il ruolo di *D.P. Officer*. A tal proposito, merita ricordare la norma di riferimento nel nostro Codice Privacy, come modificato dal D.lgs. 101/2018: l'art. 2-*quaterdecies* recita "1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

by design o *privacy by default*[24], che rappresentano anche l'insieme generale degli obblighi gravanti sui *controllers* e sui *processors*, cioè sul Responsabile e/o sull'Incaricato del trattamento dei dati personali.

Inoltre, merita ricordare anche l'art. 17 GDPR, che finalmente dà una disciplina omogenea in tutto il territorio europeo del cd. Diritto all'oblio[25].

Un ultimo elemento merita d'esser menzionato: il meccanismo di cooperazione tra Autorità Garanti di Stati Membri differenti[26]. Nel caso in cui la tutela dei dati personali, per così dire, travalichi i confini di uno Stato Membro ed entri nella sfera di competenza di uno o più Stati Membri, operano le regole di cooperazione degli artt. 60-62 GDPR, per le quali la *Lead Supervisory Authority*, l'Autorità Garante principale (cioè quella che è tenuta prevalentemente a vigilare sul trattamento dei dati personali in questione), dovrà collaborare con le altre Autorità Garanti coinvolte. Norme di incentivo per lo scambio di informazioni e la reciproca assistenza tra Autorità Garanti nazionali, onde agire e reagire in modo comune (utili, soprattutto, nella tutela dei dati personali presenti su internet o nei *Social Networks*, per esempio). In caso di contrasto tra le stesse, risolverà la controversia, con una propria decisione, la *European Data Protection Board* (un'Autorità Garante europea di nuova istituzione, *ex* artt. 68-76 GDPR, composta dai vertici di ciascuna Autorità nazionale, con poteri anche di indirizzo e coordinamento)[27].

3.1. Il quadro normativo della Certificazione, gli artt. 42 e 43 del GDPR

Uno dei principi cardine del GDPR è la trasparenza nel trattamento dei dati personali (artt. 12 e ss. del Regolamento), la quale è rivolta soprattutto verso i Responsabili e gli Incaricati del trattamento stesso. Corollario di tale principio è il meccanismo della *certification* (comprensivo, più in generale, di Certificazioni, Sigilli e Marchi di protezione dei dati personali), volto a consentire agli interessati di valutare rapidamente il livello di protezione dei dati personali. Le norme chiave relative alla Certificazione (e *de relato* a tutti gli strumenti certificatori sopra richiamati) sono l'art. 42 e 43 del GDPR (all'interno del più generale Capo IV). Ma la sua comprensione più profonda

[24] Si veda F. GIOVANNELLA, cit., 181: nel primo caso si intendono le misure tecniche e organizzative necessarie ad assicurare l'attuazione del GDPR; nel secondo caso si intendono i limiti entro (e non oltre) i quali i dati personali possono essere trattati dai gestori degli stessi.

[25] Si veda F. GIOVANNELLA, cit., 194 ss.

[26] Il *Considerando* n. 124 parla soltanto di cooperazione tra Stati Membri. Si veda P. VOIGT, cit., 198; Commissione Europea, *A framework for the free flow of non-personal data in EU*, Plus Media Solutions, Official News, 22 Giugno 2018.

[27] P. VOIGT, cit., 197.

passa preventivamente dallo scopo precipuo (e vago, al contempo) che mira a perseguire, espresso dal *Considerando* numero 100[28].

La *ratio essendi* di tutti gli strumenti certificatori (così come della Certificazione) è costituita dal raggiungimento dell'obiettivo di *trasparenza* (proprio del GDPR)[29] da parte degli enti pubblici o privati che gestiscano e/o operino su dati personali, in modo da tutelare ed informare più efficacemente i Titolari degli stessi nel loro impiego di prodotti e servizi[30].

A mente dell'art. 42.1 GDPR, gli Stati Membri, le loro Autorità Garanti per la Privacy, la EDP Board (v. *supra*) e la Commissione Europea sono chiamati ad incentivare l'impiego degli strumenti certificatori (per gli scopi suddetti) ed adattarli alle reali possibilità (economiche e gestionali) degli enti pubblici o privati (Pubbliche Amministrazioni o Società, per esempio)[31] che trattano dati personali. Lo scopo di tale attività di *soft law* è direttamente collegato al *meccanismo certificatorio*: come spiega il comma successivo, gli strumenti certificatori (come definiti dalla normativa di *soft law*) offrono ai *controllers* e ai *processors* la possibilità di dimostrare *volontariamente* la loro osservanza delle norme e il raggiungimento degli obiettivi del GDPR[32]. Ciò, come si vedrà, permette agli enti pubblici o privati il duplice vantaggio di innescare una positiva concorrenza economica tra *competitors* di uno stesso settore, da una parte, e di rassicurare il consumatore nel servizio o nel prodotto che gli viene dato, dall'altra. Tuttavia, il procedimento di adempimento degli obblighi del GDPR non si esaurisce di certo qui, con una mera dichiarazione del privato o del pubblico di rispettare la normativa europea. È proprio qui che si innesta il cd. *Procedimento certificatorio*[33].

Purtroppo, però, il GDPR non stabilisce (agli artt. 42 e 43) alcuna regola specifica per il suo sviluppo in concreto; esso definisce soltanto alcuni principi

[28] Testualmente: "Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di Certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi".

[29] Si veda il *Considerando* n. 58; in dottrina, P. VOIGT, cit., 38, 88 e 141; E. LACHAUD, 2016, cit., 817.

[30] Si veda E. LUCCHINI GUASTALLA, cit.; V. CUFFARO, *Il Diritto europeo sul trattamento dei dati personali*, in *Contratto e Impresa*, 2018, 3, 1098; E. LACHAUD, cit., 2016.

[31] Si veda il *Considerando n. 28*; in dottrina, P. LAUE, J. NINK, S. KREMER (a cura di), *Selbstregulierung, Technischer und Organisatorischer Datenschutz; Verarbeitung durch Dritte und im Ausland*, in *Das neue Datenschutzrecht in der betrieblichen Praxis*, Nomos, Baden-Baden, I ed., 2016.

[32] Ciò vale anche per gli enti extra-UE ma che, per le ragioni viste sopra, sono soggetti comunque al GDPR. Resta il dubbio che l'art. 3 GDPR possa essere applicabile anche a società che abbiano sede fuori dall'UE e che trattino dati di cittadini UE ed extracomunitari insieme. Si veda, su questo, E. LACHAUD, 2016, pag. 817, nota 18. Si ricordi, infine, che il GDPR non distingua tra *controller* e *processor*, come spiega la dottrina: P. VOIGT, 2018, cit., 80-82.

[33] Come definito in dottrina, P. VOIGT, 2018, cit., 77-78, a proposito di *Certification Procedure*. Altra dottrina, E. PELINO, in L. BOLOGNINI, E. PELINO, cit., 79, parla di *meccanismi di certificazione*.

fondamentali[34]. Infatti, è proprio qui che entra in gioco un meccanismo interessante di cooperazione verticale tra la Commissione Europea e le Autorità Garanti degli Stati Membri (e non quindi i loro Governi o Parlamenti). In base agli artt. 42.5 e 43. 8-9 GDPR, la Commissione determinerà nello specifico, attraverso *delegated acts*, i requisiti degli strumenti certificatori; le Autorità nazionali, invece, definiranno i loro criteri generali. Si stabilisce, inoltre, che i *modelli* di Certificazione potranno essere forniti dalle singole Autorità Garanti degli Stati Membri (e quindi in modo del tutto eterogeneo, nonostante il tentativo di uniformità del Regolamento stesso), oppure dai cd. *Certification Bodies*[35]. Quanto alla scelta di questi ultimi, l'art. 43.1 GDPR rimette al legislatore nazionale la scelta tra "uno o entrambi" i seguenti soggetti: l'Autorità di controllo competente, ossia il Garante per la protezione dei dati personali; ovvero, l'organismo nazionale di accreditamento designato in virtù del Reg. (CE) n. 765/2008, conformemente allo standard EN-ISO/IEC 17065/2012, che dovrà osservare i requisiti aggiuntivi stabiliti dall'Autorità di controllo.

A completamento di quanto sopra accennato, la Certificazione si configura nel GDPR come volontaria e realizzata secondo un *transparent process*. In base all'art. 42.6 GDPR, per ottenere una Certificazione, il Responsabile e/o l'Incaricato devono fornire all'Autorità Garante, o al *Certification Body*, con un proprio rapporto, tutte le informazioni rilevanti e permettere gli accessi (alle proprie strutture interne) necessari alla verifica del rispetto dei requisiti fondamentali della Certificazione stessa. La Certificazione può essere così concessa per un periodo limitato di tre anni e può essere sempre rinnovata qualora l'ente rispetti ancora i requisiti per possederla[36].

Com'è facile intuire, il raggiungimento degli obiettivi di garanzia del rispetto degli obblighi comunitari e di tutela del consumatore dipende essenzialmente dalla sua localizzazione. Infatti, potendo i singoli Stati Membri definire modelli certificatori differenti, con criteri e requisiti differenti, le società o gli enti pubblici che trattino dati personali in UE e nel mondo (di cittadini UE) daranno in concreto una attuazione (irragionevolmente) difforme delle norme del GDPR. Forse, considerando la puntigliosità dello stesso Regolamento, sarebbe stato meglio che il Regolamento avesse fornito un unico modello europeo di Certificazione (o sigillo, o marchio), con uguali criteri per tutti i *controllers* o *processors* (ossia, i Responsabili o gli Incaricati).

[34] P. LAUE, J. NINK, S. KREMER (a cura di), cit., sul *Considerando* n. 27.

[35] In base all'art. 43 GDPR sono autorità indipendenti, o società private, accreditate dalle Autorità Garanti *e* dalla EDP Board per un periodo (rinnovabile e revocabile) di 5 anni, sulla base di una serie di criteri, espressi dal comma 2. Si veda P. VOIGT, 2018, cit., 78.

[36] P. VOIGT, 2018, cit., 78; E. LACHAUD, 2016, cit., 818.

Poiché al momento manca un modello unico di Certificazione, spetterà alla Commissione Europea crearne uno.

3.2. Uno sguardo alla normativa interna

Il nostro Codice Privacy, come modificato dal D.lgs. 101/2018, ai sensi dell'art. 2-*septiesdecies*, opta per la seconda soluzione, fatta salva la possibilità per il Garante di assumere direttamente (con deliberazione pubblicata sulla G.U. della Repubblica Italiana), in caso di grave inadempimento dei compiti dell'Ente di Accreditamento (*i.e.* Accredia), l'esercizio delle sue funzioni, anche con riferimento a una o più categorie di trattamenti[37].

Accredia è stata istituita (quale Ente unico nazionale) in virtù del Decreto del Ministro dello sviluppo economico del 22 dicembre 2009. Rispetto a questa, riassumendo, il Garante: vigila sul corretto adempimento da parte dell'Ente; assume, come detto, *ex officio* le funzioni dell'Ente, nel caso in cui ravvisi un inadempimento grave del medesimo; esercita, con propri atti, un'attività di *moral suasion* prima di arrivare alla misura predetta[38].

3.3. Conseguenze e benefici derivanti dall'ottenimento di una Certificazione

C'è da specificare subito un elemento piuttosto importante: la dichiarazione di conformità alle norme del GDPR, emanata dall'ente pubblico o privato, non ha alcun valore giuridicamente vincolante, né genera alcuna responsabilità (da violazione) in capo agli stessi soggetti che la producano; al più, saranno responsabili gli Organismi Indipendenti di Certificazione, i c.d. *Certification Bodies*, come Accredia[39].

La Certificazione, come ribadisce certa dottrina, resta meramente una *autocertificazione* che non ha conseguenze giuridiche: l'unico effetto che produce, per certo, è la creazione di una *presunzione di conformità* alle norme del GDPR (ma solo di ciò che viene certificato). Anche per questo la stessa Certificazione è molto difficile da inquadrare all'interno di un ordinamento giuridico[40].

[37] Testualmente, l'art. 2-*septiesdecies* del Codice Privacy, così recita: "1. L'organismo nazionale di accreditamento di cui all'articolo 43, paragrafo 1, lettera b), del Regolamento è l'Ente unico nazionale di accreditamento, istituito ai sensi del Regolamento (CE) n. 765/2008, del Parlamento europeo e del Consiglio, del 9 luglio 2008, fatto salvo il potere del Garante di assumere direttamente, con deliberazione pubblicata nella Gazzetta Ufficiale della Repubblica italiana e in caso di grave inadempimento dei suoi compiti da parte dell'Ente unico nazionale di accreditamento, l'esercizio di tali funzioni, anche con riferimento a una o piu' categorie di trattamenti". Per il suo commento, si veda E. PELINO, in L. BOLOGNINI, E. PELINO, cit., 80.

[38] Si veda E. PELINO, in L. BOLOGNINI, E. PELINO, cit., 79-80.

[39] E. LACHAUD, 2016, cit., 823; P. VOIGT, 2018, cit., 79.

[40] La ricerca dottrinale è ancora ben lungi dall'esser definitiva su questo: si veda E. LACHAUD, 2016, cit., 823 (in particolare la nota n. 119). Manca nella dottrina italiana una chiara posizione sul punto. Accredia, sul proprio sito (https://www.accredia.it/servizi-accreditati/certificazioni/,

Per di più, in conseguenza della suddetta presunzione di conformità si genera un intoppo giuridico di non poco conto. Infatti, per espressa previsione del Regolamento (art. 43 comma 1 in combinato disposto con l'art. 25.3 GDPR), l'Autorità Garante nazionale, dopo aver ricevuto l'autocertificazione, emetterà una propria dichiarazione con la quale afferma che l'ente (autocertificatosi) stia veramente adempiendo agli obblighi del Regolamento. In alternativa, qualora l'ente sia stato certificato da un organismo indipendente di Certificazione (*Certification Body*, ovvero attraverso un c.d. *auditor*[41]), l'Autorità Garante verificherà se quest'ultimo ha rispettato i criteri di Certificazione (nazionali ed europei, v. *supra*) nel garantire la Certificazione all'ente che ha vagliato[42]. Si capisce che la maggior parte del lavoro e delle responsabilità graveranno sulle Autorità Garanti nazionali.

Tuttavia, vi sono anche conseguenze positive, di rilievo extra-giuridico, per un ente che possieda una Certificazione di conformità al GDPR[43], sia a livello interno che esterno. Per esempio, la Certificazione potrebbe rassicurare dipendenti e sindacati che l'ente stia tutelando in modo adeguato i loro dati personali; oppure, nel rapporto con *competitors*, avere una Certificazione siffatta potrebbe rappresentare un fiore all'occhiello per l'ente stesso, favorendolo nella concorrenza e sul mercato globale, sia in termini di immagine che di *business*[44].

Ma la conseguenza, se vogliamo, più importante per una società o per un organo dello Stato, che abbia una Certificazione *ex* GDPR, è rappresentata dall'art. 83.2 (lett. J) del Regolamento stesso: le sanzioni amministrative, irrogabili dalle Autorità Garanti, vengono attenuate in base ad una serie di elementi, tra cui proprio il possedere una Certificazione (o l'aver aderito a dei

consultato il 15/03/2019), definisce la Certificazione attraverso la descrizione dei suoi scopi: "Le certificazioni sotto accreditamento assicurano la conformità di sistemi, processi, prodotti, servizi e persone ai requisiti fissati dalle norme e dagli standard internazionali. Le certificazioni garantiscono il rispetto da parte di professionisti, imprese e organizzazioni pubbliche, dei requisiti previsti dalle norme e dagli standard internazionali riguardo la conformità di prodotti, servizi, processi, sistemi e persone".

[41] *Auditor* è un soggetto dipendente dell'Ente Unico nazionale di Accreditamento, che esercita in nome e per conto di quest'ultimo, le attività dello stesso. Riferirsi all'*auditor* equivale riferirsi indifferentemente sia all'Ente Unico nazionale di Accreditamento che ai suoi dipendenti, che agiscono in virtù di un rapporto di immedesimazione organica con l'Ente. Ciò sarà vero fintanto che Accredia, dal punto di vista italiano, sia l'unico soggetto chiamato a svolgere le funzioni di accreditamento e di certificazione.

[42] Qui si aprono due possibili soluzioni giuridiche per l'inquadramento del procedimento certificatorio del Regolamento, per cui v. *ultra*.

[43] Ma il discorso potrebbe essere esteso a qualsiasi tipo di Certificazione p.e. di standard qualitativo (come le ISO 9001 e simili).

[44] Si veda la lunga analisi fatta da E. LACHAUD, 2016, cit., 819-820.

codici di condotta) [45]; oltretutto, se l'ente è certificato, la sanzione amministrativa potrà essere inflitta solo in caso di violazione della normativa GDPR, ma esclusivamente localizzate nelle attività certificate[46]. Chiaramente, però, l'Autorità Garante, in presenza di violazioni *gravi* del GDPR commesse da un soggetto pubblico o privato (certificato da un *auditor* riconosciuto), può ordinare la revoca immediata della Certificazione stessa (come *extrema ratio*)[47].

3.4. Possibili interpretazioni del procedimento certificatorio

L'organismo indipendente, ovvero il cd. *Third party accredited auditor*, è una figura centrale nel meccanismo di Certificazione. Ai sensi dell'art. 43, c. 4-6 GDPR, egli è tenuto a collaborare proattivamente col soggetto pubblico o privato da certificare (pur evitando ogni sorta di collusione), per realizzare poi la dichiarazione di conformità al GDPR del soggetto stesso (il c.d. *Data Protection Impact Assessment*). A livello formale parrebbe un procedimento piuttosto lineare. Il problema è che, nonostante il Regolamento chieda che il procedimento certificatorio si sviluppi in modo trasparente (v. *supra*), il GDPR non specifica le condizioni di tale trasparenza[48]. Non è dato neanche sapere se l'ente possa avere comunque una Certificazione senza collaborare con l'*auditor*, né se e come debba intervenire un giudice adito in caso di asserite violazioni della privacy da parte dell'ente stesso[49].

In più, c'è da considerare anche il fatto che, stando al tenore letterale degli artt. 42 e 43 GDPR, l'ente pubblico o privato ha la facoltà di emanare unilateralmente una propria autocertificazione, in attesa di essere poi vagliato *in personam* dall'Autorità Garante o da un *auditor*, verificando così la veridicità o meno dell'autocertificazione stessa. Né il GDPR, né il nostro Codice Privacy, come modificato nel 2018, pongono divieti in tal senso. Ed è proprio per questo che non è facile comprendere di che genere sia il meccanismo di Certificazione, né tantomeno il Certificato finale emanato dall'Ente Unico nazionale di Accreditamento (Accredia, per l'Italia)[50].

[45] Si consideri anche, preliminarmente, che il mancato rispetto delle norme del GDPR potrebbe condurre a sanzioni amministrative pari a 10 milioni di euro o al 2% del *fatturato annuale* della società (art. 83.4 GDPR).

[46] P. VOIGT, 2018, cit., 79.

[47] Danneggiando anche l'immagine dell'ente stesso. Questa *extrema ratio* fornisce un potere di veto materiale all'Autorità Garante nazionale rispetto agli organismi indipendenti di Certificazione, sulla base del disposto dell'art. 58.2 (lett. H) del GDPR. La casistica di operatività è limitata a casi gravissimi (ma non impossibili), come la collusione fraudolenta tra l'organismo e l'ente da certificare.

[48] E. LACHAUD, 2016, cit., 817.

[49] Si veda l'art. 42.3 GDPR.

[50] È bene qui distinguere la Certificazione, intesa come procedimento, ed il singolo atto conclusivo dello stesso, cioè un Certificato, un Marchio o un Sigillo.

In dottrina sono emerse due possibili interpretazioni[51], la di cui disamina può essere utile ad inquadrare al meglio la Certificazione nel nostro ordinamento.

La prima possibilità è che la Certificazione sia un procedimento dichiarativo volontario (e facoltativo) realizzato da un *auditor* esterno ed accreditato, sulla base dei requisiti e criteri imposti dall'Autorità Garante nazionale (nonché dalla disciplina di *soft law* di cui sopra). Detto altrimenti, l'*auditor* si reca presso l'ente pubblico o privato, lo vaglia attentamente e produce una dichiarazione, dalla quale emerga che l'ente stesso risulti conforme (o meno) alla normativa europea e nazionale sulla *privacy* (dalle regole del GDPR a quelle di *soft law*). La dichiarazione di conformità (*Data Protection Impact Assessment*) viene poi "consegnata" all'ente sotto forma di Certificato, Marchio o Sigillo (garanzia di tutela dei dati personali che gestisce); sarà infine lo strumento certificatorio ad esperire tutta la sua efficacia esterna ed interna per l'ente certificato (di cui *supra*).

Una seconda possibilità, al contrario, parte dal presupposto che la Certificazione in sé sia soltanto una *attestazione di conformità*[52]; il procedimento certificatorio potrebbe apparir così un processo attraverso il quale un terzo *auditor* (accreditato ed indipendente), in seguito alla produzione di un'autocertificazione da parte di un ente pubblico o privato, dà una garanzia scritta che l'autocertificazione stessa risulti conforme a determinati requisiti imposti (dalla normativa europea, nazionale e di *soft law* in materia di *privacy*). In altre parole, per distinguere la seconda interpretazione dalla prima, il meccanismo funzionerebbe grossomodo così: l'ente pubblico o privato emana innanzitutto una autocertificazione di conformità; in un secondo momento l'*auditor* la controlla per verificare che corrisponda al vero (sulla base della normativa di *hard and soft law* vigente in materia); infine, lo stesso *auditor* produce un'attestazione certificatoria definitiva dell'adeguatezza dei meccanismi (propri dell'ente) di tutela dei dati personali (sotto forma di Certificato, Sigillo o Marchio).

In definitiva, nella prima soluzione è l'*auditor* a certificare (e ad assumersi tutte le responsabilità del caso), sollevando così l'ente da molti oneri e responsabilità[53]; nella seconda soluzione, invece, è l'ente ad emanare una propria autocertificazione, che verrà in seguito controllata, approvata e certificata dall'*auditor*[54].

[51] Entrambe le soluzioni sono state riprese dalle tesi di E. LACHAUD, 2018, cit., 245-246 (sulla base di P. EIJLANDER, 2003, cit., 12).

[52] Questo è l'approccio enunciato nell'ISO 17000:2004-*Conformity Assessment*, *Vocabulary and general principles*, subclause 5.5.

[53] Ma è la soluzione ovviamente più costosa per l'ente pubblico o privato.

[54] Tale soluzione, diciamo, di compromesso, permette di ripartire le responsabilità tra i due protagonisti del procedimento certificatorio.

Come e quando poi debba intervenire l'Autorità Garante nazionale in questo macchinoso ed oscuro procedimento, non emerge chiaramente né dal GDPR, né dal riformato D.lgs. 196/2003. Ma che essa debba intervenire su di una autocertificazione dell'ente, o su un'attestazione certificativa dell'*auditor*, la sua attività di verifica necessaria consisterà nel valutare in concreto che le dichiarazioni rese corrispondano al vero, al fine di irrogare eventuali sanzioni amministrative[55]. Ciò che cambia è il diverso grado di responsabilità amministrativa o penale per l'ente e/o per l'*auditor*[56].

È facile comprendere che il perno di tutto il procedimento certificatorio, da qualsiasi prospettiva lo si guardi, sia la *self-regulation*, promanante da un'autocertificazione di un ente (pubblico o privato, Responsabile o Incaricato che sia), ovvero da un *Assessement* di un terzo *auditor* (su quanto abbia verificato riguardo all'ente e i dati personali che questi gestisce).

Data l'importante novità introdotta dal GDPR, cui il nostro Codice fatica ad adeguarsi, è necessario tentare un inquadramento giuridico dello strumento certificatorio, così come della *self-regulation*.

3.5. La Certificazione e la *self-regulation* nell'ordinamento italiano

Come riconosce certa dottrina[57], è ancora incerto l'inquadramento della Certificazione nel nostro ordinamento; ma non è neanche ben chiaro se questa possa essere identificata come *self-regulation* o come *public regulation*[58]; anche perché lo studio sulla sua natura giuridica è ancora poco approfondito. È chiaro però che, seguendo i due possibili schemi visti nel paragrafo precedente, la Certificazione può esser ricondotta sia all'una che all'altra tipologia d'atto. Complica però le cose una terza tipologia, di sintesi, che appare molto complicata da inquadrare nel nostro ordinamento (la cd. *Co-regulation*).

In via generale si può affermare che la Certificazione introdotta dal GDPR si configuri come uno strumento facoltativo, a metà tra la teoria

[55] Ai sensi dell'art. 154-*ter*, c. 1, del Codice Privacy, come modificato nel 2018, "1. Il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali". Nel nostro Codice, inoltre, vi sono esempi di sanzioni amministrative (artt. 166 e ss.), nonché penali per le violazioni delle regole di trattamento dei dati sensibili (p.e. art. 50, c. 1, ultima parte). Peraltro, ai sensi dell'art. 144, c. 1, "Chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento".

[56] Oltre alle singole ipotesi richiamate nella nota precedente, si pensi ai fatti di reato puniti, per esempio, ai sensi degli artt. 479-480 c.p. (falso ideologico del pubblico ufficiale, come l'*auditor* o l'ente pubblico), piuttosto che dell'art. 483 c.p. (falso ideologico del privato); o, addirittura, ai sensi del combinato disposto di tali norme con l'art. 48 c.p. (che configurerebbe una falsità ideologica per induzione, con la responsabilità dell'autore mediato). Sulla punibilità per un'autocertificazione mendace, si veda R. BARTOLI, *Reati contro la fede pubblica*, Giappichelli, Torino, 2011.

[57] L. BOLOGNINI, E. PELINO, cit., 79-80.

[58] Si veda E. LACHAUD, 2018, cit., 251.

dell'imposizione e controllo (*command and control*) della Direttiva 95/46/CE[59], e gli strumenti di *self-regulation*, nati a margine di un contesto giuridico fumoso, prosperati sin dagli inizi del nuovo millennio senza un sicuro livello di affidabilità e garanzia per gli autori e per i destinatari.

Ciò, con l'arrivo del GDPR, ha fatto pensare alcuni[60] ad una nuova tipologia di produzione del diritto, collocata entro una *new hierarchy in the enforcement of the law*. Sì perché, da una parte, i *controllers/processors* possono volontariamente dichiararsi conformi alle norme del GDPR (senza reali conseguenze giuridiche "a monte")[61]; dall'altra, qualora dovessero essere certificati da un terzo *auditor*, al più potrebbero patire delle conseguenze contrattuali, da inadempimento degli obblighi nascenti dai rapporti negoziali con l'*auditor* stesso. Tutto questo farebbe pensare ad una natura prettamente privatistica e contrattualistica della Certificazione.

Tuttavia, ai sensi dell'art. 42, c. 7 del GDPR, l'autorità giudiziaria o le Autorità Garanti nazionali (sulla base delle normative interne degli Stati Membri) potrebbero intervenire in qualsiasi momento contro i *controllers*, i *processors* e, persino, gli *auditors*, qualora risulti evidente che non vi siano più i presupposti per possedere la Certificazione, ovvero qualora venga accertato che gli stessi stiano violando le regole europee e nazionali di settore. Chiaramente, ciò tende a sbilanciare la Certificazione su un piano più propriamente pubblicistico.

È evidente che, *sic rebus stantibus*, la natura giuridica della Certificazione resti molto incerta. Oltretutto, gli Stati Membri e le Autorità Garanti nazionali potrebbero creare modelli di Certificazione differenti (da Stato a Stato), attuando la riserva legislativa dell'art. 42.1 GDPR, ma complicando ulteriormente le cose.

Come poi questi diversi schemi possano essere ricondotti a figure già esistenti nel diritto interno, oppure ad altre create *ex novo*, resta un mistero nelle mani del legislatore (nazionale e sovranazionale). Ecco perché qualcuno ha definito la *omogeneizzazione* dei vari schemi di Certificazione a livello europeo un vero *incubo*[62]. Per la Commissione Europea, oltretutto, trovare la formula giusta per avere un'*unica Certificazione europea* potrebbe essere davvero un rompicapo. Tuttavia, per le imprese private, di qualsiasi

[59] J. JORDANA e D. LEVI-FAUR, *The politics of regulation in the age of governance*, in *Handbook on the Politics of Regulation*, Edward Elgar Publishing, vol. III, 2004.

[60] E. LACHAUD, 2018, cit., 251.

[61] Ai sensi dell'art. 42.4 GDPR. Salvo, ovviamente, responsabilità penali o amministrative "a valle".

[62] B. HEAVNER, M.R. JUSTUS, *World-wide Certification-Mark Registration A Certifiable Nightmare*, Bloomberg Law Reports, 2009, come letto da E. LACHAUD, 2018, cit., 252.

dimensione, e per gli enti pubblici, la presenza di un unico modello certificatorio europeo sarebbe di gran lunga auspicabile[63].

Se però provassimo a mettere da parte le due interpretazioni sulla natura giuridica della Certificazione (v. *supra*), una soluzione di sintesi potrebbe essere trovata. Una sintesi il cui inquadramento giuridico potrebbe apparire forse lontano dalle classificazioni del nostro ordinamento[64].

Si tratta del modello della *co-regulation*, miscuglio tra dimensione privatistica e pubblicistica, nel quale l'autocertificazione del *controller* o del *processor* ha rilievo pubblico, tanto da generare su di questi una responsabilità ulteriore, nascente da una "quasi-governamental function", che può essere sindacata dall'autorità giudiziaria o dall'Autorità Garante per la Privacy[65]. Un modello nel quale lo standard (di tutela dei dati personali da parte di *controllers/processors*) assume un rilievo socio-politico e culturale, oltre che costituzionale, visto che la Certificazione dovrebbe assicurare il rispetto di alcuni diritti fondamentali (quali il diritto alla privacy, alla corrispondenza segreta e personale, ecc.). Qui sarà cruciale il ruolo della Commissione Europea, *in primis*, e delle Autorità Garanti nazionali, *in secundis* (ai sensi dell'art. 43, c. 8 del GDPR), nello stabilire gli standard *concreti* di tutela dei dati personali. Ma sarà ancora più importante l'opera degli organismi indipendenti (per l'Italia, di Accredia) nel comprendere se e come vengano rispettati questi standard da parte dei soggetti, Responsabili e/o Incaricati (che andranno a certificare), collaborando eventualmente con gli *stakeholders* e necessariamente con le Autorità Garanti nazionali[66].

Qui sta il cuore della *co-regulation*: da un atto privatistico, emanato sulla base della normativa di settore (europea e nazionale, di *hard law* come di *soft law*), ad una collaborazione proattiva con svariati organismi pubblici, nell'ottica di rendere effettivi i diritti costituzionali relativi alla sfera personale (e *personalissima*) dei cittadini UE. In dottrina[67], viene definita anche *Monitored self-regulation*, poiché la Certificazione, pur restando inizialmente un atto privatistico senza particolari onerosità, viene costantemente controllata da organismi indipendenti e pubblici (come le Autorità Garanti nazionali e gli *auditor* accreditati), proprio per la rilevanza costituzionale che essa va ad assumere nel garantire l'attuazione del diritto alla privacy.

[63] Favorendo davvero la massima integrazione e cooperazione a livello europeo degli stessi soggetti, insieme alla certezza del loro rispetto degli standard richiesti dal GDPR.

[64] I modelli c.d. ibridi, di cui *ultra*, sono stati pensati da T. BARTLEY, *Certification as a mode of social regulation*, Department of Sociology Indiana University Bloomington, 2010, e da D. LEVI-FAUR, ult. cit.

[65] V.A. LOCONTO e L. BUSCH, *Standards, techno-economic networks, and playing fields: performing the global market economy*, in *Rev. Int. Polit. Econ.*, 2010, 17, 509-510.

[66] Così E. LACHAUD, 2018, cit., 254.

[67] *Ibi supra*.

Se così fosse, la Certificazione, introdotta dal GDPR per la tutela dei dati personali, aprirebbe una nuova frontiera per gli ordinamenti e, in particolare, per i legislatori (nazionali) che non conoscono il modello della *co-regulation* per la produzione di effetti giuridici. Infatti, la *Monitored self-regulation*, seguendo uno schema che, in Italia, potrebbe rassomigliare alla Segnalazione Certificata di Inizio Attività (S.C.I.A.)[68]. La S.C.I.A., come noto, nei casi previsti dai c. 1 e 2 dell'art. 22 del d. P. R. n. 380/2001, è un atto di un soggetto privato e non di una PA, che ne è invece destinataria e preposta al controllo di conformità dell'atto alla realtà sostanziale, e non costituisce, pertanto, esplicazione di una potestà pubblicistica (*ex multis*, Cons. St. sez. VI, 9 febbraio 2009, n. 717 sulla natura giuridica della D.I.A.); la sua mancanza, poiché titolo abilitativo esclusivo per avviare i lavori, non comporta l'applicazione di sanzioni penali ma solo amministrative (art. 37, c. 6, del d. P. R. n. 380/2001)[69]. Benché vi possano essere delle discrasie tra la Certificazione e la S.C.I.A., un siffatto meccanismo di produzione degli effetti giuridici, a metà tra privato e pubblico, potrebbe consentire alle autorità pubbliche di definire *soltanto* i moduli, i modelli e i criteri della Certificazione privatistica, delegando poi ai privati la concreta *attuazione* di tali regole, verificata in ultima istanza dagli *auditors* e/o dalle Autorità Garanti[70]. Dopo tutto, questo era lo stesso obiettivo per il raggiungimento del quale furono creati gli standard qualitativi *ISO 9001*[71].

3.6. Qualche rilievo pratico

Al di là di certe obiezioni fatte sopra riguardo all'oscurità del testo normativo in esame, vi sono ulteriori conseguenze critiche da affrontare, seppur accennate, che fanno ritenere il percorso di riforma del GDPR incompiuto[72].

Un primo rilievo, in parte richiamato sopra, riguarda il procedimento certificatorio e i soggetti che lo animano: da una parte, il Responsabile e/o l'Incaricato del trattamento del dato personale autocertifica il proprio rispetto

[68] P. TANDA, *I reati urbanistico-edilizi*, Wolters Kluwer-Cedam, Padova, V ed., 2019, 73 ss.; per l'evoluzione dell'istituto, R. DAMONTE, *L'evoluzione normativa della denuncia di inizio attività lavori alla luce della legislazione regionale e della recente giurisprudenza amministrativa*, in *Riv. Giur. Ed.*, 2004, 95 ss.

[69] Le similitudini però finiscono qui, nel senso che la S.C.I.A. muove da uno schema di produzione degli effetti giuridici di "norma-fatto-effetto", mentre la Certificazione, mera facoltà di un ente pubblico o privato (che *voglia* certificare o far attestare il suo standard adeguato di tutela dei dati personali), segue probabilmente lo schema di "norma-potere sull'*an*-effetto". Sul punto, si veda P. TANDA, cit., 78-79.

[70] *Ibi supra*; E. LACHAUD, 2018, cit., 254.

[71] T. HAVINGA, P. VERBRUGGEN, *Hybridisation of Food Governance: Trends Types and Results*, in *Panel Hybridization of RegGov: Trends, Types and Results of PublicPrivate Interaction ECPR on Standing Group on Regulatory Governance Conference*, Barcelona 25–27 Giugno 2014.

[72] Si veda l'analisi compiuta da E. LACHAUD, 2016, cit., 818-821.

del GDPR, del Codice Privacy (interno) e del *soft law* in materia; dall'altra, l'*auditor* esterno verifica che ciò corrisponda al vero, al reale. Detto questo, si pone il problema di eventuali responsabilità penali (o amministrative) per i due soggetti, nascenti, per esempio, dalla consumazione di reati come la falsità del privato o del pubblico ufficiale ideologica o materiale (artt. 479 e ss. c.p.). Per dare un'idea di quanto affermato, se l'autocertificazione fosse falsa ideologicamente e l'*auditor* la desse per veritiera, la dottrina penalistica più accorta[73] porterebbe a ritenere che responsabile, *ex* art. 480 c.p. (in combinato disposto con l'art. 48 c.p.), sia l'autore della stessa, se l'*auditor* ne controlla il contenuto; ovvero, *ex* art. 483 c.p., se questi non controlla affatto il suo autore. Secondo la giurisprudenza più recente[74], si potrebbe invece ritenere responsabile l'autore della dichiarazione, a prescindere dall'attività di controllo effettiva dell'*auditor*. Ancora, forse, è prematuro dare una soluzione certa.

Questo ci porta al secondo problema: ammesso che il procedimento certificatorio che fa perno sull'autocertificazione dell'ente sia un meccanismo veloce, flessibile e dilazionatorio di un intervento eventuale dell'autorità giudiziaria (e dello Stato), esso potrebbe però perdere di affidabilità generale nel suo sviluppo. Molto dipenderà dal grado di garanzia di controllo effettivo offerto dall'*auditor* così come dall'Autorità Garante.

Vi sono anche delle problematiche di ordine economico. Anzitutto riguardo alla concorrenza tra società private, così come tra Stati Membri. Come si è detto, possedere un determinato marchio qualitativo e, ad oggi, anche del rispetto della normativa di settore (privacy), permette ad una società certificata di avere un'immagine migliore, più attraente per investitori e clienti, rispetto ai *competitors* che ne siano sprovvisti; il fatto che tutto però ruoti attorno ad una autocertificazione (solo successivamente controllata da *auditor* e/o dall'Autorità Garante) non è molto rassicurante per l'effettiva tutela del diritto alla privacy, ben potendo il soggetto (pubblico o privato) fare affermazioni "gonfiate" o, peggio, non veritiere.

A ciò si aggiunge anche il fatto che i vari modelli di autocertificazione potrebbero essere differenti da Stato a Stato dell'Unione fintanto che l'Unione stessa non adotti un proprio unico modello (regolamentato) di Certificazione, generando una corsa alla maggior garanzia o alla maggior spregiudicatezza[75].

[73] Si veda R. BARTOLI, cit.

[74] cfr. Cass. pen., sez. V, n. 12400/2015; Cass. pen., sez. II, n. 28076/2012; Cass. Sez. Un. 28.6.2007, Scelsi, in *Cass. Pen.*, 2008, pagg. 93 e ss.; anche in *Dir. pen. Proc.*, 2008, pagg. 999 e ss., con nota di C. DE PELLEGRINI, *Quando la falsità del privato comporta la falsità dell'atto pubblico a contenuto dispositivo?*, *ivi*, pag. 1002.

[75] Si veda E. LACHAUD, 2016, cit., 824.

Oltretutto, al fianco dell'*auditor pubblico* (Accredia), vi sono già anche dei privati (accreditati dall'*auditor pubblico* stesso o dall'Autorità Garante per la protezione dei dati personali), che spesso collaborano (in virtù di rapporti negoziali con gli enti da vagliare e certificare), come consulenti (i c.d. *privacy managers*). Un certo tipo di *vicinitas* è ben lungi dalla garanzia di effettiva tutela dei diritti dei consumatori, così come dei cittadini UE coinvolti, con risvolti sull'economia e sul lavoro.

Il secondo rilievo di tipo economico, ed anche conclusivo, riguarda gli alti costi del meccanismo certificatorio[76]. La valutazione di un consulente per la privacy, che permetta all'ente di mettersi in regola con la normativa di settore, prima che arrivi l'*auditor pubblico* (come Accredia) a verificare la situazione concreta, potrebbe costare migliaia di euro; ed è una spesa che andrebbe sostenuta annualmente. Se poi, successivamente a tale investimento, l'ente dovesse incorrere in qualche violazione della tutela dei dati personali (anche per fatto a lui non imputabile, come per esempio in occasione di un *attacco hacker*), l'ente stesso subirebbe ulteriori conseguenze (negative): da una parte, il danno all'immagine e le spese per il ripristino dello *status quo ante*; dall'altro, eventuali sanzioni amministrative e/o penali (per esempio, previste dal D.lgs. 196/2003, dopo le modifiche apportate nel 2018).

Questo ci porta ad una considerazione finale: gli enti che vogliano (per *core business*) esser certificati, investiranno certamente per tale scopo; chi non ne sentisse il bisogno (per svariati motivi) non investirà affatto per ottenere la Certificazione, ed attuerà la normativa di settore in misura ridotta, forse soltanto cambiando il modulo dell'informativa del trattamento dei dati personali[77].

4. Conclusioni sullo stato dell'arte

Il cammino del GDPR e del nuovo procedimento certificatorio è appena iniziato; dai rilievi critici più marcati si deve prendere spunto per migliorare una disciplina riformatrice che ha innovato già di molto rispetto alla vecchia normativa della Direttiva 95/46/CE. Ciò che manca evidentemente è, da una parte, un incentivo forte, anche a livello economico e fiscale, della Certificazione delle PMI e dei grandi enti pubblici (come per esempio, le nostre ASL) e, dall'altra, l'omogeneità dei modelli certificatori in tutta l'Unione Europea.

Dal punto di vista giuridico, sarà essenziale per la Commissione Europea (e per gli Stati Membri) definire chiaramente (anche con strumenti di *soft law*)

[76] *Ibi supra*.

[77] Purtroppo, a causa dei costi da sostenere per l'adeguamento alla normativa di settore, per le PMI sarà molto difficile attuare la stessa *in concreto*, col rischio di esser ulteriormente schiacciate dalla concorrenza di chi si può permettere l'investimento nella Certificazione.

i rapporti che debbono intercorrere tra Responsabili, Incaricati, Titolari, Autorità Garante, *auditor* pubblici e privati.

Dopo tutto, gli strumenti certificatori degli standard di garanzia della *privacy* possiedono una funzione cruciale in un mondo iper-connesso e globalizzato come quello attuale: consentire l'*effettiva* tutela dei dati personali.