Evoluzione del diritto cantonale della protezione dei dati – *quo vadis*?

GIORDANO COSTA

Indice

I. Premessa

Sono trascorsi 35 anni dall'introduzione della legge cantonale sulla protezione dei dati[1]. Da allora, la protezione dei dati si è trovata confrontata con dinamiche tecnologiche e con strategie di digitalizzazione che hanno influenzato

[1] Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP; RL 163.100).

in modo importante lo Stato, nelle prassi e nel diritto. Si è così assistito a una trasposizione di un'importante parte delle attività pubbliche e delle rispettive elaborazioni di dati personali nella sfera virtuale, dando luogo a un complesso di prassi con considerevoli implicazioni sui diritti del cittadino. La nuova impostazione del diritto cantonale della protezione dei dati – prescritta dal diritto internazionale, che è stato oggetto di revisioni fondamentali negli ultimi anni – prevede un'estensione dei diritti delle persone interessate e degli obblighi dei titolari delle elaborazioni di dati, così come l'ampliamento delle facoltà di applicazione della legge e di sanzionamento. Lo scopo ultimo consiste nel creare un quadro giuridico più solido per il diritto alla riservatezza nella sfera digitale dello Stato[2].

II. Vincoli internazionali per la Confederazione e i Cantoni

A. Consiglio d'Europa

Il Consiglio d'Europa ha adottato il 18 maggio 2018 la modernizzazione della Convenzione STE 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e del suo Protocollo aggiuntivo STE 181 dell'8 novembre 2001 concernente le autorità di controllo e i flussi internazionali di dati, adottando il rispettivo Protocollo d'emendamento (in seguito: STE 108+). Il 21 novembre 2019, il Consiglio federale ha firmato la STE 108+, aderendo così alla sua modernizzazione[3]. La ratifica è stata approvata dal Parlamento svizzero durante la sessione parlamentare estiva del 19 giugno 2020[4]. La Svizzera ha ratificato la STE 108+ principalmente per ragioni inerenti alla tutela dei diritti dell'uomo, ma anche per ragioni economiche (agevolazione della comunicazione transfrontaliera

2 Consid. 10 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati); vedi anche Frei, *Datenschutz-Grundverordnung und die Schweiz*, pag. 80 segg; Rosenthal, *Das neue Datenschutzgesetz*, pag. 3.

3 Messaggio concernente l'approvazione del Protocollo di emendamento del 10 ottobre 2018 alla Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale, FF 2020 531.

4 Sessione parlamentare estiva 2020, 19 giugno 2020, 19.068 – Protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale – Convenzione; sulla ratifica del Protocollo di emendamento della Convenzione STE 108 da parte della Svizzera, vedi anche Frei, *Datenschutz-Grundverordnung und die Schweiz*, pag. 84.

di dati) e per non compromettere la decisione di adeguatezza dell'Unione europea circa il diritto svizzero sulla protezione dei dati. La ratifica è vincolante anche per i Cantoni, che sono obbligati ad adempiere i nuovi requisiti previsti dalla STE 108+ e a recepirli nel loro diritto.

B. Unione Europea

L'Unione europea ha, dal canto suo, emanato due nuovi atti normativi, uno generale sulla protezione dei dati (Regolamento [UE] 2016/679), l'altro specifico alla protezione dei dati nel settore della polizia e del giudiziario penale (Direttiva [UE] 2016/680). Ambedue i nuovi atti normativi hanno iniziato a espletare pienamente i loro effetti giuridici a partire dal 25 maggio 2018, dopo un periodo transitorio di adeguamento di due anni. Perseguono essenzialmente gli scopi di garantire la protezione dei diritti e delle libertà fondamentali nella società digitale, la lotta al terrorismo e alla criminalità, assicurando nel contempo la libera circolazione delle rispettive informazioni tra le autorità competenti, nonché l'ottimizzazione dell'economia tramite la libera circolazione dei dati e l'aumento della competitività del mercato grazie a nuove attività economiche legate alla società digitale.

1. Regolamento (UE) 2016/679 (GDPR)

L'Unione europea ha riveduto la propria legislazione sulla protezione dei dati, sostituendo innanzitutto la Direttiva 95/46 CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con il nuovo Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati (in seguito: GDPR – General Data Protection Regulation). A differenza della STE 108+ e della Direttiva [UE] 2016/680, la Svizzera non è vincolata al GDPR, poiché quest'ultimo non costituisce parte integrante dell'*acquis* di Schengen, né rappresenta un trattato internazionale in altro modo vincolante per la Svizzera[5]. Non è quindi tenuta a recepirlo e attuarlo. La Confederazione, così come i Cantoni, intendono tuttavia allineare il proprio diritto anche al GDPR, per non compromettere la decisione dell'Unione europea di adeguatezza del diritto svizzero della protezione dei dati e, quindi, in particolare, per non compromettere gli interessi economici del nostro

[5] Rimane riservata l'applicazione del GDPR qualora siano adempiute le condizioni poste dall'art. 3 GDPR (ambito di applicazione territoriale).

Paese e la rispettiva, libera circolazione dei dati[6]. La decisione di adeguatezza dell'Unione europea garantisce, infatti, all'economia di Paesi terzi come la Svizzera il libero scambio di merci e servizi e dei relativi dati personali con l'Unione, senza ulteriori condizioni quali autorizzazioni o convenzioni sulla protezione dei dati, direttive sulla protezione dei dati interne alle imprese svizzere, o altro[7].

2. Direttiva (UE) 2016/680

L'Unione ha abrogato la Decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale e ha promulgato in sua vece la Direttiva (UE) 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. La Direttiva (UE) 2016/680 è parte dell'acquis di Schengen. Deve dunque essere attuata anche dalla Confederazione e dai Cantoni, per evitare di compromettere gli accordi di Schengen, in particolare l'accesso delle autorità svizzere di polizia al sistema d'informazione di Schengen SIS. Confederazione e Cantoni sono stati chiamati a adattare il loro diritto entro due anni dalla notifica, avvenuta il 1° agosto 2016. La Svizzera ha notificato l'accettazione della Direttiva il 1° settembre 2016. Per adempiere al più presto le condizioni della Direttiva 2016/680, il Parlamento svizzero ha trattato le rispettive norme di attuazione separatamente dalla revisione totale della LPD, adottandole il 28 settembre 2018. La rispettiva legge federale sulla protezione dei dati nell'ambito dell'applicazione dell'acquis di Schengen in materia penale è entrata in vigore il 1° marzo 2019[8].

La corretta attuazione e applicazione della direttiva (UE) 2016/680 viene riesaminata in tutti gli Stati Schengen circa ogni cinque anni nell'ambito di un processo di valutazione. La terza valutazione Schengen della Svizzera è stata

6 Frei, *Datenschutz-Grundverordnung und die Schweiz*, pag. 83. Sui criteri alla base della decisione di adeguatezza, vedi anche, della stessa autrice: Frei, *Revision des Datenschutzgesetzes*, pag. 7. Sulle intenzioni della Svizzera di adeguarsi al GDPR, vedi in particolare Rosenthal, *Das neue Datenschutzgesetz*, pag. 2 segg, 5 [10].

7 Vedi art. 45 GDPR. Sul tema, vedi in particolare Frei, *Revision des Datenschutzgesetzes*, pag. 7 e Powell, pag. 2 e 3.

8 LPDS; RS 235.3. Dal canto suo, la revisione totale della legge federale sulla protezione dei dati è stata adottata dal Parlamento il 25 settembre 2020. L'entrata in vigore del nuovo diritto in materia di protezione dei dati è prevista per il 1° settembre 2023; il Consiglio federale non ha ancora adottato la decisione formale necessaria a tal fine.

effettuata nel 2018[9]. A seguito dell'adozione della relazione di valutazione, il 7 marzo 2019 il Consiglio dell'UE ha emesso una serie di raccomandazioni per l'eliminazione delle carenze individuate ("raccomandazioni Schengen")[10].

c. Principali novità del diritto internazionale

Peculiarmente ai diritti delle persone, il diritto internazionale prevede in particolare le seguenti modifiche:

- diritto di accesso: sono ampliate le categorie d'informazioni riguardanti l'elaborazione di dati da fornire all'interessato in caso di richiesta di accesso ai propri dati; inoltre, è previsto che il diritto di accesso non può essere limitato senza motivazione (ad esempio, il rischio di vanificare un perseguimento penale in atto, o la necessità di protezione di altre persone);
- diritto alla portabilità dei dati: su richiesta, il titolare del trattamento deve mettere a disposizione dell'interessato i suoi dati personali su adeguato supporto portatile;
- diritti di rettifica e di cancellazione: sono da garantire senza ingiustificato ritardo;
- diritto alla limitazione del trattamento: in alcuni casi previsti dalla legge, l'interessato può ottenere la limitazione del trattamento dei suoi dati personali; il titolare potrà soltanto conservare i dati, senza possibilità di ulteriori operazioni su di essi;
- diritto di opposizione: l'interessato può opporsi a qualsiasi trattamento che lo riguarda, riservata l'esistenza di un interesse preponderante o di una legge;
- diritto all'oblio: nel caso in cui dati personali sono stati trasmessi a terzi, il titolare dovrà informarli della richiesta di rettifica, cancellazione o distruzione dei dati effettuata da parte della persona interessata;
- diritto alla comunicazione di una violazione dei dati personali: il titolare del trattamento è tenuto a comunicare all'interessato le violazioni dei dati personali suscettibili di presentare un rischio elevato per i suoi diritti e le sue libertà.

9 Oltre alla Confederazione, per la valutazione era stato selezionato il Canton Lucerna.

10 Vedi raccomandazioni in: Durchführungsbeschluss des Rates zur Festlegung einer Empfehlung zur Beseitigung der 2018 bei der Evaluierung der Anwendung des Schengen Besitzstands im Bereich des Datenschutzes durch die Schweiz festgestellten Mängel, 7 marzo 2019 (‹https://data.consilium.europa.eu/doc/document/ST-7281-2019-INIT/de/pdf›).

Per quanto riguarda gli obblighi dei titolari di elaborazioni di dati, il diritto internazionale prevede in particolare:

- obbligo della valutazione d'impatto: il titolare dell'elaborazione è tenuto ad analizzare i rischi per i diritti e a implementare le misure di minimizzazione, da sottoporre all'autorità di vigilanza in materia di protezione dei dati, qualora l'elaborazione di dati presenti un rischio elevato per i diritti e le libertà delle persone;
- principio della responsabilità (o obbligo della prova del rispetto della protezione dei dati): il titolare dell'elaborazione è attivamente responsabile di agire in conformità con il diritto sulla protezione dei dati e, in particolare, di comprovare che l'elaborazione avviene in conformità con quest'ultimo;
- principio dell'approccio basato sui rischi: maggiore è il rischio per i diritti e le libertà fondamentali, maggiori sono le responsabilità del titolare del trattamento, che dovrà in particolare mettere in atto misure di sicurezza adeguate ai rischi e meccanismi e sistemi di controllo del rispetto del diritto;
- principio della protezione dei dati fin dalla progettazione (*Privacy by design*) e per impostazione predefinita (*Privacy by default*): le garanzie della protezione dei dati devono essere prese in considerazione sin dalla progettazione dei prodotti e dei servizi;
- principio della trasparenza: il titolare dell'elaborazione è tenuto a fornire all'interessato informazioni di dettaglio relative all'elaborazione (in particolare, alla raccolta) di dati che lo concernono (informazione attiva); l'informativa deve essere facilmente accessibile e di facile comprensione, in particolar modo nel caso di informazioni a minori; non deve necessariamente sempre essere individuale (può essere collettiva);
- obbligo di auto-segnalazione: il titolare deve notificare all'autorità di controllo indipendente e, in taluni casi, anche alla persona interessata, le violazioni dei dati personali da lui perpetrate, senza ingiustificato ritardo, affinché l'autorità di controllo possa esercitare le sue mansioni legali;
- obbligo d5el registro delle elaborazioni di dati: ogni organo pubblico che elabora dati personali deve tenere un registro delle proprie attività di elaborazione;
- obbligo di un'autorità di controllo pienamente autonoma e indipendente: l'autorità di controllo deve agire in piena autonomia e indipendenza e disporre di tutte le risorse umane, tecniche e finanziarie necessarie per l'effettivo adempimento dei suoi compiti legali e deve avere la facoltà di prendere decisioni vincolanti impugnabili e di pronunciare sanzioni amministrative.

III. Evoluzione del diritto della protezione dei dati in Ticino

A. Brevi cenni storici

Come già anticipato, anche i Cantoni devono adattare le loro leggi sulla protezione dei dati alle nuove esigenze poste dal diritto internazionale, e più precisamente negli ambiti statali e parastatali cantonali[11]. Le modifiche devono trasporre la STE 108+ e la Direttiva (EU) 2016/680, attuare le raccomandazioni Schengen e tenere adeguatamente conto, più in generale, del GDPR. Nel febbraio del 2017, la Conferenza dei Governi cantonali ha messo a disposizione dei Cantoni una guida sulla riforma europea della protezione dei dati e sulla modernizzazione della Convenzione del Consiglio d'Europa STE 108, con indicazione degli adeguamenti minimi delle leggi cantonali necessari per raggiungere l'adeguatezza con il diritto superiore. Con Risoluzione governativa 5564 del 13 dicembre 2017, il Consiglio di Stato ha, successivamente, costituito il gruppo di lavoro per la revisione della LPDP, il quale ha consegnato il progetto di revisione totale alla Cancelleria di Stato il 17 febbraio 2020[12]. Il 17 maggio 2023, il Consiglio di Stato ha licenziato il messaggio relativo alla revisione totale della LPDP[13].

B. Principali adeguamenti della legge cantonale ticinese sulla protezione dei dati (LPDP)

Qui di seguito vengono esposte le principali proposte di modifiche della LPDP, ad esclusione di quelle di entità minore, in particolare relative ai

11 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati (FF 2017 5939, 5985). Vedi anche Powell, pag. 4. Da notare che nonostante la standardizzazione operata dal diritto internazionale, restano numerose questioni che sono disciplinate in modo diverso nei Cantoni. Questa circostanza potrebbe porre ulteriormente l'accento sull'obiettivo a medio termine di una legge sulla protezione dei dati uniforme in tutta la Svizzera per gli enti pubblici della Confederazione e dei Cantoni proposto da alcuni esperti.

12 Attualmente, secondo la lista attualizzata di privatim, la Conferenza degli Incaricati svizzeri della protezione dei dati, concernente lo stato di avanzamento dei lavori di revisione delle leggi cantonali (‹https://www.privatim.ch/fr/›), sono circa la metà i Cantoni che hanno già completato la revisione delle proprie leggi sulla protezione dei dati, rispettivamente il cui processo legislativo si trova in uno stadio avanzato (tra questi, AG, AR, BL, BS, GL, LU, NE, SG, SH, SZ, ZG e ZH). Negli altri Cantoni i lavori di revisione del diritto cantonale sulla protezione dei dati non è ancora stato avviato, oppure, come in Ticino, è ancora nelle fasi preliminari o intermedie (tra questi, AI, BE, FR, GE, GR, JU, NW, OW, SO, TI, UR ,VD e VS).

13 ‹https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/M8281_Revisione_totale_LPDP.pdf›.

rafforzamenti dei diritti già esistenti (ad esempio, le modifiche relative all'esecuzione del diritto di rettifica, che dovrà avvenire entro un termine regionevole, oppure relative al diritto di accesso, che riprenderà esplicitamente nella legge il contenuto delle informazioni da fornire all'interessato). Parte delle modifiche imposte dal diritto superiore (ad esempio, il diritto alla portabilità dei dati) verranno attuate nel regolamento d'esecuzione della LPDP[14], motivo per cui non verranno esposte in questo contributo.

1. Campo di applicazione

Le attuali norme sul campo di applicazione della LPDP (art. 2 e 3) vengono scomposte in tre nuove disposizioni (Campo di applicazione *a)* materiale, *b)* istituzionale e personale, *c)* procedurale; art. 2–4 progetto LPDP), per garantire maggiore chiarezza giuridica e per meglio integrarvi le necessarie modifiche imposte dal diritto superiore. Per quanto riguarda in particolare il campo di applicazione istituzionale e personale, la Conferenza dei Governi cantonali propone di escludere lo Stato quando agisce come un privato[15], suggerendo di prevedere esplicitamente la competenza dell'Incaricato cantonale della protezione dei dati per quanto riguarda la vigilanza, da eseguire secondo le specifiche norme cantonali. Di conseguenza, quando un organismo statale o parastatale non agisce nell'ambito del compito pubblico affidatogli, ma è soggetto alla concorrenza economica, le rispettive elaborazioni di dati sono sottoposte alla legislazione federale sulla protezione dei dati, sulla corretta applicazione delle quali vigila l'Incaricato cantonale in aplicazione della LPDP[16].

2. Definizioni[17]

a) Dati personali delle persone giuridiche

Il diritto internazionale ha lo scopo di proteggere le persone fisiche dai pericoli che possono derivare dal trattamento dei dati personali. I dati sulle persone giuridiche non sono, invece, protetti. Con la revisione del diritto federale sulla protezione dei dati, il legislatore ha sottratto dal concetto di dati personali i dati delle persone giuridiche, principalmente a ragione del fatto che la

[14] Regolamento di applicazione alla legge cantonale sulla protezione dei dati personali (RLPDP; RL 163.110).

[15] Tale esclusione è già prevista dall'attuale art. 2 cpv. 3 LPDP.

[16] Sul campo di applicazione della nuova LPDP, vedi: ‹https://www4.ti.ch/can/sgcds/pd/generalita/revisione-totale-lpdp›.

[17] Sulle definizioni in generale, vedi: ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Definizioni.pdf›.

protezione della personalità delle persone giuridiche (comunque, di rilevanza pratica limitata) è già garantita da diverse leggi speciali, ad esempio dalla tutela della personalità di cui agli articoli 28 segg. del Codice civile[18], dal diritto della concorrenza[19] e della proprietà intellettuale (in particolare, legislazione federale sulla protezione dei marchi[20]), dal segreto bancario dell'art. 47 della legge sulle banche[21], dai segreti aziendali di cui all'articolo 162 del Codice penale[22] e dalle norme sulla protezione dei dati di cui agli art. 143 segg. del Codice penale[23]. Il legislatore federale ha però deciso, nell'ambito della trasparenza e dell'informazione pubblica, di continuare a proteggere i dati delle persone giuridiche in relazione all'accesso ai documenti ufficiali[24].

La problematica principale legata all'esclusione dei dati personali delle persone giuridiche dal concetto di dati personali risiede nel fatto che la base legale richiesta dall'art. 36 cpv. 1 Cost. per la violazione di diritti fondamentali tramite l'elaborazione di dati personali – diritti garantiti, in ambito di tutela della privacy, anche alle persone giuridiche – non è più data. Ciò, a ragione del fatto che le disposizioni sul trattamento dei dati personali nelle leggi speciali offrono – in seguito all'esclusione della protezione dei dati personali delle persone giuridiche – una base per il trattamento dei soli dati delle persone fisiche. Per questo motivo, il legislatore federale ha dovuto introdurre nella legge sull'organizzazione del Governo e dell'Amministrazione del 21 marzo 1997[25] una serie di disposizioni che disciplinano il trattamento di dati di persone giuridiche da parte di organi federali, le quali sostituiscono, *de facto*, le norme contenute nella LPD.

Contrariamente al legislatore federale, in Ticino, così come in altri Cantoni (ad esempio, ZH, SZ), si è scelto di mantenere la protezione delle persone giuridiche nella LPDP (art. 5 cpv. 1 progetto LPDP)[26]. Riprendere lo stesso meccanismo internazionale e federale a livello cantonale avrebbe infatti implicato la necessità di inserire delle norme ad hoc di protezione dei dati

18 Codice civile svizzero del 10 dicembre 1907 (CC; RS 210).

19 Legge federale contro la concorrenza sleale del 19 dicembre 1986 (LCSI; RS 241).

20 Legge federale sulla protezione dei marchi e delle indicazioni di provenienza (Legge sulla protezione dei marchi; LPM; RS 232.11).

21 Legge federale sulle banche e le casse di risparmio dell'8 novembre 1934 (Legge sulle banche; LBCR; RS 952.0).

22 Codice penale svizzero del 21 dicembre 1937 (CP; RS 311.0).

23 POWELL, pag. 5 segg. [8–11]; RUDIN, pag. 60; ROSENTHAL, *Das neue Datenschutzgesetz*, pag. 7 [19].

24 POWELL, pag. 5 segg.

25 LOGA; RS 172.010.

26 Altri Cantoni, come ad esempio AG, AI, BL, GL, SG e ZG, hanno seguito l'approccio federale.

personali delle persone giuridiche nel diritto settoriale cantonale. Ciò avrebbe comportato una certa inflazione normativa, oltre a creare una certa insicurezza giuridica.

b) Dati genetici

Nella lista di dati meritevoli di particolare protezione secondo la LPDP, vengono introdotti i dati genetici (art. 5 cpv. 2 lett. e progetto LPDP)[27]. Questi ultimi sono informazioni sul patrimonio genetico di una persona ottenute attraverso un esame genetico; ne fa parte anche il profilo del DNA[28]. Per essere considerati dati sensibili, questi dati devono necessariamente basarsi su un processo tecnico che permetta l'identificazione e l'autenticazione univoca della persona.

c) Dati biometrici

Alla stessa stregua di quanto prevede il diritto federale e internazionale, anche i dati biometrici vengono ora esplicitamente elencati nella lista di dati meritevoli di particolare protezione della LPDP (art. 5 cpv. 2 lett. f progetto LPDP)[29]. Si tratta di quei dati personali che, grazie a un trattamento tecnico specifico, si ricavano da caratteristiche fisiche o comportamentali uniche e identificative di ciascuna persona fisica[30]. Fanno parte di questa categoria di dati, ad esempio, le impronte digitali, la specifica conformazione fisica della mano o del volto, dell'iride o della retina, la firma grafometrica (ovvero quella firma elettronica effettuata su apposito supporto mediante un gesto fisico in tutto coincidente con quello utilizzato per firmare su carta), nonché il timbro e la tonalità della voce, a partire dal momento che permettono di identificare una persona in modo univoco. I dati biometrici sono dati personali nella misura in cui possono essere associati a una persona identificata o identificabile[31].

d) Profilazione

Il diritto internazionale[32] ha introdotto il concetto di profilazione, che viene ora ripreso dalla LPDP come nuova tipologia di elaborazione di dati

27 Vedi art. 4 cfr. 13 GDPR e art. 3 cfr. 12 Direttiva 2016/680.

28 Vedi art. 3 lett. l della legge federale sugli esami genetici sull'essere umano dell'8 ottobre 2004; LEGU; RS 810.12.

29 Vedi art. 4 cfr. 14 GDPR e art. 3 cfr. 13 Direttiva 2016/680.

30 Nel caso di normali fotografie, questa premessa non è data.

31 Vedi Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati; FF 2017 5939.

32 Art. 4 cfr. 4 GDPR e 3 cfr. 4 Direttiva 2016/680.

soggetta alla legge (art. 5 cpv. 9 progetto LPDP). La profilazione è intesa come il processo di valutazione di determinate caratteristiche di una persona stilata sulla base di dati personali ottenuti tramite elaborazione automatica e finalizzati soprattutto all'analisi e alla previsione di interessi, performance lavorative, condizioni economiche e di salute, comportamento, luogo di dimora e mobilità, ecc., al fine di prendere misure e decisioni commisurate al soggetto. La profilazione si ha quindi in presenza di 3 elementi: 1. un trattamento automatizzato, 2. eseguito su dati personali, 3. con lo scopo di valutare aspetti personali di una persona fisica per potervi adattare una determinata reazione. Non si tratta quindi di mero tracciamento dell'interessato, finalizzato alla sola giornalizzazione di eventi, senza uno specifico scopo. La profilazione deve adempiere alle stesse condizioni poste all'elaborazione di dati meritevoli di particolare protezione (segnatamente, una base legale in senso formale).

Ad oggi, i Cantoni hanno inserito la profilazione nelle loro leggi, come previsto dal diritto europeo e hanno rimosso anche il concetto di profilo della personalità, benché tale rimozione non sia imposta dal diritto superiore. Effettivamente, la minaccia ai diritti fondamentali che deriva dai profili di personalità quale insieme di dati va relativizzata, se non è il risultato di una profilazione, vale a dire in particolare se non costituisce un'ipotesi su interessi, caratteristiche, preferenze, bisogni, caratteristiche, ecc., della persona. In questo senso, alcuni Cantoni qualificano i risultati della profilazione come profili della personalità e li assoggettano alle stesse condizioni valide per l'elaborazione di dati personali particolarmente sensibili[33]. Così, sia il processo di profilazione, sia i suoi risultati, beneficiano di una protezione speciale. In Ticino, il concetto di profilo della personalità non è esplicitamente previsto dalla LPDP, ma nell'attuazione pratica della legge viene tutelato.

3. Condizioni qualificate per l'elaborazione di dati meritevoli di particolare protezione

La Conferenza dei Governi cantonali propone di prevedere nelle leggi cantonali sulla protezione dei dati le esigenze qualificate per l'elaborazione di dati personali meritevoli di particolare protezione, come la base legale formale, o la necessità assoluta per l'adempimento di compiti legali. Il Ticino ha introdotto già nel 2016 l'obbligo di basi legali per le elaborazioni sistematiche di dati personali, che devono essere di rango formale in caso di dati meritevoli di particolare protezione (art. 6 cpv. 1 LPDP)[34].

[33] Ad esempio, AI e GL.

[34] Messaggio n. 7061 del 18 marzo 2015: ‹https://www4.ti.ch/fileadmin/CAN/SGCDS/ICPD/PDF/DIRITTO_TI/m7061_01.pdf›.

4. Obbligo d'informazione sulla raccolta di dati personali

Fra i principi che reggono l'elaborazione di dati personali vi è, nuovo, l'obbligo di informare le persone interessate in occasione della raccolta di dati (art. 10 progetto LPDP)[35].Tale obbligo costituisce una concretizzazione del principio di buona fede di cui all'art. 9 Cost. e del principio di trasparenza dell'attività amministrativa. L'obbligo di informare implica che l'informazione sia chiara, possibilmente esaustiva e non contraddittoria. L'obbligo sussiste soprattutto laddove i dati non siano raccolti presso la persona interessata. L'informazione ha lo scopo di migliorare la qualità dei rapporti tra lo Stato e il cittadino e di rafforzare la consapevolezza della persona interessata circa i suoi diritti. Senza la necessaria informazione, quest'ultima potrebbe non venire a sapere che i suoi dati vengono trattati. Questa trasparenza e questa sensibilizzazione costituiscono obiettivi fondamentali perseguiti dalla LPDP. Con l'obbligo di informare vi è del resto un generale allineamento al GDPR, alla Direttiva UE 2016/680, alla STE 180+ e alle raccomandazioni della Conferenza dei Cantoni. La revisione della LPDP, allineandosi con quanto sopra, indica quali informazioni minime debbano essere concretamente fornite alla persona interessata. Si tratta, in particolare, dell'identità (il cognome e nome) e le coordinate di contatto del titolare dell'elaborazione, delle finalità dell'elaborazione dei dati e del loro eventuale cambiamento e delle categorie di dati elaborati, dei destinatari dei dati e dei diritti delle persone interessate.

5. Obbligo della valutazione d'impatto sulla protezione dei dati

Le nuove disposizioni del diritto superiore[36] prescrivono la realizzazione da parte dell'organo responsabile di un'analisi d'impatto sulla protezione dei dati (o valutazione del rischio). Si tratta dell'obbligo d'individuazione preventiva dei rischi per le libertà e i diritti fondamentali degli interessati e delle misure specifiche per attenuare o eliminare tali rischi. In altre parole, si tratta di identificare i rischi in tempo utile in modo da poter adottare adeguate misure di mitigazione. L'analisi deve contenere almeno una descrizione delle procedure dell'elaborazione di dati prevista, una valutazione dei rischi per i diritti fondamentali delle persone interessate e l'esposizione e valutazione delle misure prese per rimediarvi. Costituisce la preparazione da parte dell'organo responsabile delle condizioni per dare seguito all'obbligo della prova del rispetto della protezione dei dati. Alla stessa stregua del legislatore federale, il Ticino risponde a questa esigenza introducendo una nuova

[35] Cfr. art. 14 GDPR. Sull'obbligo d'informazione dell'art. 10 progetto LPDP, vedi: ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Obbligo_d_informazione.pdf›.

[36] Art. 27 Direttiva 2016/680; art. 35 GDPR; art. 10 § 2 STE 108+.

disposizione (art. 13 progetto LPDP), secondo il quale il titolare dell'elaborazione realizza una valutazione d'impatto relativa alla protezione dei dati quando v'è un rischio elevato di violazione della protezione dei dati[37]. Ciò è il caso quando l'elaborazione permette una valutazione sistematica e globale per un vasto numero di interessati entro un perimetro geografico più o meno ampio (elaborazione su larga scala), segnatamente, nel settore pubblico, in caso di:

- elaborazioni automatizzate finalizzate ad assumere decisioni che producono effetti giuridici;
- interconnessione di banche dati, combinazione o raffronto d'informazioni;
- videosorveglianza del demanio pubblico;
- riconoscimento facciale;
- tracciamento di movimenti;
- videosorveglianza o geolocalizzazione nell'ambito del rapporto di lavoro;
- elaborazioni di dati di un ospedale relative ai pazienti;
- elaborazioni di un'azienda di trasporti pubblici relative agli utenti (tracciamento attraverso titoli di viaggio);
- elaborazioni concernenti soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, migranti, richiedenti l'asilo).

La valutazione d'impatto deve contenere almeno:

- la descrizione delle elaborazioni previste, delle rispettive finalità, della base giuridica e del soggiacente interesse legittimo;
- la valutazione della necessità e proporzionalità dell'elaborazione in relazione alla finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati.

Se sono evidenziati rischi particolari, il titolare del trattamento dovrà consultare preventivamente l'autorità di controllo indipendente (incaricato della protezione dei dati), presentando, tra l'altro, la valutazione d'impatto. Non per ogni progetto di elaborazione di dati deve essere allestita un'analisi dei rischi di uguale ampiezza[38].

[37] È chiaro che la valutazione dell'esistenza di un rischio elevato richiede comunque anche una certa, minima analisi del rischio. Sulla valutazione d'impatto secondo l'art. 13 progetto LPDP, vedi: ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Spiegazioni__Valutazione_ProtezioneDati.pdf›; ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Formulario_valutazione_LPDP.pdf›.

[38] Powell, pag. 8 segg.

6. Obbligo della prova del rispetto della protezione dei dati

Il diritto cantonale ticinese sulla protezione dei dati allarga le responsabilità per l'elaborazione di dati all'obbligo di tutti gli attori coinvolti di essere in grado, in ogni momento, di provare che rispettano la protezione dei dati (art. 8 cpv. 1 progetto LPDP)[39]. Il diritto superiore parla a questo proposito di sistema di gestione della protezione dei dati (SGPD)[40]. La prova può essere data ad esempio quando vengono adottati specifici standard di sicurezza, ad esempio le norme ISO relative alla gestione della qualità (ISO 9001) e alla sicurezza dell'informazione (ISO 27001).

7. Obbligo dell'autosegnalazione

Il diritto internazionale ha introdotto l'obbligo di segnalare le violazioni della sicurezza dei dati all'autorità di controllo della protezione dei dati[41]. La violazione della sicurezza dei dati comprende, tra l'altro, la perdita di supporti dati, l'accesso di terzi non autorizzati ai sistemi informatici, le violazioni della sicurezza dei dati a causa di vizi tecnici e la divulgazione di dati non autorizzata. Il diritto internazionale richiede generalmente una segnalazione all'autorità di controllo per ogni violazione, a meno che sia improbabile che essa comporti un rischio per i diritti fondamentali degli interessati.

Il Canton Ticino ha introdotto l'obbligo della notifica della violazione della protezione dei dati (art. 16 progetto LPDP)[42]. La norma prevede che la violazione della protezione dei dati è data quando la compromissione della sicurezza dei dati ha comportato la soppressione definitiva o la perdita di dati, la loro modifica o la loro divulgazione non intenzionale o illecita o la loro accessibilità da parte di terzi non autorizzati. La notifica deve avvenire entro congruo termine[43]. Non sussiste l'obbligo di notifica quando la violazione

39 Sull'art. 8 cpv. 1 progetto LPDP vedi: ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Obbligo_della_prova_del_rispetto_della_protezione_dei_dati_-_Copia.pdf›.

40 Vedi in particolare art. 10 cfr. 1 STE 108+.

41 Art. 30 segg. Direttiva 2016/680; art. 33 segg. GDPR; art. 7 STE 108+.

42 Sull'obbligo dell'autosegnalazione vedi: ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Spiegazioni__Segnalazione_DatiPersonali.pdf›; ‹https://www4.ti.ch//fileadmin/CAN/SGCDS/ICPD/PDF/LPDP/Formulario_segnalazione_dati_personali.pdf›.

43 La Direttiva 2016/680 (art. 30 cfr. 1) e il GDPR (art. 33 cfr. 1) prevedono un periodo di segnalazione generale non superiore a 72 ore dal momento del rilevamento della violazione della sicurezza dei dati. La Confederazione e finora tutti i Cantoni hanno rinunciato a un termine di segnalazione così rigoroso, ma chiedono che il rapporto sia presentato il prima possibile. Questa soluzione lascia il margine necessario per l'esame del singolo caso, anche se una segnalazione entro 72 ore dalla conoscenza della violazione può sembrare spesso ragionevole o addirittura necessaria.

della protezione dei dati non presenta verosimilmente dei rischi per i diritti della personalità e le libertà fondamentali della persona interessata.

La norma prevede inoltre che il titolare dell'elaborazione deve informare anche le persone interessate quando le circostanze lo esigono o l'Incaricato lo chiede (diritto della persona interessata alla comunicazione di una violazione dei dati personali). Si può rinunciare in tutto o in parte all'informazione, o la si può differire, se un interesse privato o pubblico preponderante lo esige[44]. È previsto infine che il responsabile (mandatario) dell'elaborazione notifichi tempestivamente ogni violazione della protezione dei dati al titolare dell'elaborazione.

8. Obbligo dell'autorità indipendente

Nel corso degli sviluppi normativi a livello europeo, sono stati fermamente ribaditi i requisiti – già previsti dai precedenti atti normativi europei e dalla LPDP (art. 30 cpv. 2 LPDP, art. 33 cpv. 1 progetto LPDP) – di indipendenza delle autorità di controllo per la protezione dei dati personali. Il rafforzamento dell'indipendenza è anche un elemento centrale delle raccomandazioni Schengen del 7 marzo 2019 nei confronti della Svizzera.

In merito all'obbligo della completa autonomia e indipendenza dell'Incaricato della protezione dei dati, va sottolineato come essa sia la prima e imprescindibile condizione posta dal diritto europeo a tutti gli Stati parte, e quindi anche alla Svizzera e a tutti i Cantoni. Essa va pertanto riconosciuta sotto il profilo istituzionale e funzionale. Siccome imposta dal diritto superiore, fatta salva la decisione di allacciamento amministrativo dell'Incaricato, la sua autonomia non può essere considerata e declinata liberamente. La stessa procedura di nomina dell'Incaricato – poiché riconducibile a meccanismi parlamentari – accentua la centralità dell'indipendenza. La piena autonomia e indipendenza dell'Incaricato è imprescindibile ritenuto che esso esercita funzioni non riconducibili né all'apparato amministrativo, né all'attività di governo, ma alla Costituzione. L'autonomia e indipendenza dell'Incaricato – che si avvicina a quella dei giudici e si distingue dalla mera imparzialità degli altri servizi

[44] Il diritto europeo (Direttiva, art. 31, GDPR, art. 34, STE 108+, art. 7 cfr. 2) prevede l'obbligo d'informazione delle persone interessate nel caso in cui la violazione della sicurezza dei dati implichi un rischio elevato per i loro diritti e le loro libertà. Il legislatore federale segue un approccio leggermente modificato, in quanto richiede che gli interessati siano informati solo se ciò è necessario per la loro protezione o se l'IFPDT lo richiede (art. 24 cpv. 4 nLPD). In linea di principio si può quindi presumere che il legislatore federale abbia destinato le informazioni principalmente alle situazioni in cui l'interessato può prendere precauzioni per la propria protezione (ad es. modificando i dati di accesso o le password).

dell'amministrazione cantonale – si giustifica ed è imposta, come già ribadito, per le delicate e complesse funzioni svolte dallo stesso e mira a creare una funzione neutrale e riconosciuta come effettivo e credibile garante dei diritti e delle libertà fondamentali in relazione all'elaborazione di dati personali. Poiché agisce a tutela di diritti e interessi di rilievo costituzionale, l'Incaricato deve essere esente da qualsiasi tipo d'influenza, e ciò ancor più nel quadro del diritto internazionale in materia di protezione dei dati personali, recepito nel diritto federale e cantonale. Si tratta, quindi, in altre parole, di garantire le necessarie lontananze dalle dinamiche proprie del circuito amministrativo e politico al fine di evitare ogni influenza o pressione esterna – anche soltanto indiretta, segnatamente e in particolare risultante da un assoggettamento gerarchico – e assicurare credibilità. Se ciò non è il caso, l'organizzazione della protezione dei dati è lesiva dell'obbligo d'indipendenza e comporta il rischio di affievolimento delle garanzie costituzionali in questione. È necessario che l'indipendenza sia formalmente prevista dalla legge. Qualsiasi impiego secondario è anche importante per l'indipendenza dell'autorità di controllo, poiché può portare a conflitti di interesse. La direttiva (art. 42 cpv. 3) e il GDPR (art. 52 cpv. 3) vietano atti e attività incompatibili con lo svolgimento dell'incarico. Il lavoro secondario dovrebbe rimanere l'eccezione[45].

9. Competenza decisionale dell'autorità di vigilanza

Gli ordinamenti giuridici europei richiedono che l'autorità di controllo della protezione dei dati abbia il potere di emanare decisioni vincolanti in caso di violazioni della protezione dei dati[46]. Il potere di disporre come facoltà particolarmente importante per l'efficacia dell'autorità di vigilanza è sottolineato anche nelle raccomandazioni Schengen.

In Ticino, attualmente la LPDP prevede che se dai chiarimenti risulta che sono state violate prescrizioni sulla protezione dei dati, l'Incaricato raccomanda l'organo responsabile di modificare o di cessare l'elaborazione. Egli informa della raccomandazione l'autorità superiore competente. Il titolare dell'elaborazione o, se del caso, l'autorità superiore competente, dichiarano all'Incaricato, entro congruo termine definito da quest'ultimo, se intendono seguire la raccomandazione (art. 30*b* cpv. 4 e 6 LPDP). Se la raccomandazione dell'Incaricato è respinta o non le è dato seguito, in tutto o in parte, egli

[45] Gli esempi di membro di consiglio di amministrazione, di professore o giudice non sono, a priori, esclusi, ma richiedono misure adeguate per evitare conflitti di interesse. Tuttavia, garantire l'indipendenza rappresenta una sfida in particolare per i Cantoni più piccoli, a ragione del fatto che lo svolgimento della funzione di incaricato della protezione dei dati viene a volte attribuita, a tempo parziale, a un funzionario o a un mandatario esterno.

[46] Art. 47 cpv. 2 lett. b Direttiva 2016/680; art. 58 cfr. 2 GDPR; art. 15 cpv. 2 lett. c STE 108+.

può deferire la pratica all'autorità superiore competente, la cui decisione può essere impugnata anche dall'Incaricato (art. 30*b* cpv. 6 e 7 LPDP).

La revisione della LPDP prevede ora che, se una raccomandazione è respinta o non le è dato seguito, in tutto o in parte, l'Incaricato può decidere di far applicare tutta o parte della raccomandazione, se l'interesse alla sua messa in opera è preponderante. L'Incaricato può emettere direttamente una decisione se è prevedibile che il titolare dell'elaborazione rigetti la raccomandazione o non gli dia seguito (art. 38 cpv. 7 progetto LPDP).

C. Conclusioni

Riconoscendo la necessità di rafforzare i diritti fondamentali nell'era digitale, negli ultimi anni il diritto internazionale si è sviluppato in modo importante, spingendo il legislatore federale e cantonale verso la creazione di un diritto equivalente, o perlomeno avente gli stessi effetti, nei rispettivi ambiti di competenza[47]. I necessari adeguamenti legislativi avrebbero dovuto entrare in vigore entro il 1° agosto 2018, ma in Ticino, così come anche in altri Cantoni, la revisione della legislazione cantonale sulla protezione dei dati è in ritardo.

Ai ritardi legislativi nei Cantoni si aggiungono strategie e prassi di digitalizzazione che sembrano spesso andare nella direzione opposta rispetto agli attuali sviluppi legislativi. Ne è forse l'esempio più lampante il principio *Once-only*, che sta prendendo sempre più piede e che implica la raccolta di dati personali un'unica volta e la loro condivisione tra diverse entità dell'amministrazione pubblica, per diversi scopi, in nome dello sgravio burocratico delle persone coinvolte e dell'aumento dell'efficacia dell'amministrazione pubblica. Se non assoggettato a specifici limiti, il principio *Once-only* implica una contraddizione con il principio della finalità, il quale rischia di essere svuotato della sua sostanza, con i conseguenti rischi per i diritti di personalità che ne derivano[48]. La costante digitalizzazione dello Stato[49], la videosorveglianza pubblica a tappeto, il riconoscimento facciale, il tracciamento dei movimenti tramite lettura delle targhe dei veicoli, il tracciamento dettagliato dei consumi di acqua potabile e di energia elettrica, così come l'interfacciamento di banche dati e la conseguente creazione di ampi profili

47 Frei, *Revision des Datenschutzgesetzes*, pag. 25 segg.

48 Astrid Epiney/Sophia Rovelli, *Once-only et le principe de l'Etat de droit,* in: digma Schriften zum Datenrecht, Zurigo/Ginevra 2022, vol. 11, cap. 3.2.2.5, pag. 111 segg.

49 Sul tema delle strategie di digitalizzazione dello Stato, vedi tra l'altro Bruno Baeriswyl, *Fehlender digitaler Kompass*, in: digma Zeitschrift für Datenrecht und Informationssicherheit, fascicolo 1, marzo 2018, pag. 36.

della personalità, nonché altre pratiche intrusive nella sfera privata come i sopralluoghi domiciliari, sono ulteriori esempi di prassi che mettono sotto pressione la protezione dei dati.

In questo campo di tensione tra tecnologia, prassi e diritto, le forze che spingono verso la trasparenza e il controllo sempre più completo della persona appaiono oggigiorno preponderanti, a tal punto che l'essenza stessa della privacy, considerata in origine come immutabile, pare evolvere verso sempre maggiore fluidità e adattabilità, tanto da non essere più certi che tale essenza non stia effettivamente cambiando o non sia già cambiata. Di questo passo, si rischia che – in un paradossale e radicale stravolgimento delle logiche di diritto – siano improvvisamente i diritti e le libertà fondamentali a doversi giustificare nei confronti della digitalizzazione, della razionalizzazione dell'amministrazione pubblica e del controllo, e non viceversa. Vi è pertanto da sperare che il Ticino, così come gli altri Cantoni in ritardo nel loro processo legislativo di adeguamento della protezione dei dati, si ricordino del loro compito forse più importante, vale a dire la massima funzionalizzazione dello Stato alla protezione dei diritti e delle libertà fondamentali del cittadino[50]. È perciò auspicabile che la protezione dati ricopra un ruolo di maggior rilievo, non soltanto attraverso il rafforzamento legislativo, ma anche attraverso il rafforzamento della vigilanza. Ne va del nostro modello istituzionale liberale, della democrazia, dello stato di diritto, della libertà. Perché la protezione dei dati è condizione della libertà.

[50] Vedi anche RUDIN, pag. 202.