LA NUOVA LEGGE SULLA PROTEZIONE DEI DATI

20 Aprile 2023

La nuova legge sulla protezione dei dati

La revisione totale della LPD, oltre ad una sua modernizzazione, mira a adeguare la normativa svizzera ai requisiti europei in ambito di trattamento dati

Premessa

La più grande parte della revisione della nuova Legge federale sulla protezione dei dati (nLPD), si fonda sull'implementazione delle disposizioni della Convenzione 108+, le quali hanno per obiettivo una maggiore tutela delle libertà e dei diritti fondamentali delle persone fisiche in relazione all'elaborazione automatizzata dei loro dati a carattere personale aumentando il senso di responsabilizzazione (cd. principio di accountability) di coloro che trattano i dati personali. A tale fine, la nLPD ha introdotto una seria di obblighi nei confronti delle aziende (titolari del trattamento) volti a migliorare la trasparenza del trattamento dei dati personali delle persone fisiche e aumentando il senso di responsabilità del titolare del trattamento, nonché allo stesso tempo permettendo alle persone interessate di controllare i dati che le riguardano. Il tutto con un inasprimento delle disposizioni penali in caso di violazione o di inadempienze nei confronti del titolare del trattamento e, in particolare, a carico dei dirigenti, amministratori e detentori del potere decisionale in seno alle aziende (titolari del trattamento).

I. Introduzione

Dinanzi agli sviluppi europei in materia di protezione dei dati ed alla rapida evoluzione tecnologica, la revisione totale della Legge federale sulla protezione dei dati (LPD; RS 235.1) mira a:

- modernizzare l'attuale legge sulla protezione dei dati personali (di seguito descritta con l'acronimo aLPD, diversamente da quella nuova descritta con l'acronimo nLPD) e rafforzarla per fare fronte alla rapida evoluzione tecnologica;
- attuare gli impegni assunti al livello internazionale e, in particolare, ratificare il protocollo di modifica (protocollo di emendamento 223 detto anche Convenzione 108+) del testo della Convenzione 108, Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale .. La Convenzione 108 o Convenzione di Strasbourg del 1981 (RS 0.235.1) è uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali[1];
- adeguarsi al diritto europeo onde consentire anche in futuro la comunicazione transfrontaliera di dati senza necessità di fare valere le garanzie previste dagli artt. 46 a 49 Regolamento UE n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (*General Data Protection Regulation* [GDPR]) e che permetterebbe alla Svizzera di assicurarsi il rinnovo della decisione di

[1] La Convenzione 108 del Consiglio d'Europa sancisce che il trattamento o la raccolta dei dati deve avvenire rispettando i seguenti principi: *(i)* correttezza del trattamento, *(ii)* liceità del trattamento, *(iii)* finalità del trattamento, *(iv)* qualità dei dati.

adeguatezza[2] (art. 45 GDPR) di cui beneficia già dal 2000[3] e di cui il riesame è stato prorogato[4], in attesa della sentenza della Corte di Giustizia dell'Unione europea (CGUE) interpellata in seguito al reclamo pendente di Maximilian Schrems contro i trasferimenti di dati verso gli Stati Uniti d'America (USA)[5].

Dopo una descrizione dell'*iter* legislativo, il presente contributo illustrerà dapprima le principali novità della nLPD rispetto all'aLPD pertinente per il settore privato, alle quale seguirà una presentazione di alcuni obblighi delle aziende (di seguito "titolari del trattamento") volti a migliorare la trasparenza dei trattamenti dei dati personali nei confronti delle persone interessate e di alcune misure tecniche-organizzative che, oltre a prevenire/mitigare i rischi per la personalità e i diritti fondamentali delle persone interessate, sono destinate a comprovare, documentare, illustrare in maniera circostanziata e regolare l'implementazione di un processo necessario a proteggere la personalità e i diritti fondamentali delle persone interessate (cd. principio di *accountability*). Infine, verranno esposte le sanzioni penali applicabili ai sensi della nLPD nei confronti del titolare del trattamento e, in particolare, nei confronti delle persone fisiche detentrici del potere decisionale in seno al titolare del trattamento in caso di violazione di alcuni obblighi o di inadempienze.

II. L'iter legislativo

La nLPD è un progetto iniziato nel lontano dicembre 2011. Di fronte sia alla rapida evoluzione delle tecnologie che all'intensificazione dei trattamenti e diffusione dei dati con i conseguenti rischi di lesione per la personalità, l'Ufficio federale di giustizia (UFG) ha provveduto tra il 2010 e il 2011 ad una valutazione della LPD, il cui rapporto è stato approvato dal Consiglio federale in data 9 dicembre 2011[6].

---

2 La decisione di adeguatezza è un atto rilasciato dalla Commissione europea ai Paesi terzi riconosciuti "*safe*", ossia che garantiscono un livello di protezione adeguato. La decisione viene riesaminata, di solito, ogni quattro anni.

3 Decisione della Commissione europea del 26 luglio 2000 riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (art. 25 par. 6).

4 A giugno 2020, la Commissione europea ha deciso di rinviare il suo riesame della decisione di adeguatezza (cfr. OneTrust DataGuidance, EU: Commission postpones adequacy decision reviews for Switzerland and other countries, 25 giugno 2020, in: https://www.dataguidance.com/news/eu-commission-postpones-adequacy-decision-reviews-switzerland-and-other-countries [consultato il 15.02.2023]).

5 La vicenda Maximilian Schrems è iniziata nel 2013, in seguito alle rivelazioni di Edward Snowden. Schrems ha denunciato Facebook all'autorità garante della *privacy* irlandese in quanto non voleva che Facebook, la cui sede si trova in Irlanda, condividesse i suoi dati personali con Facebook Inc, la sede principale americana, i cui *server* sono collocati in USA. Di fronte alla respinta dell'autorità garante irlandese, Schrems ha adito *l'High Court* (Alta Corte, Irlandese), la quale ha sottoposto alla CGUE una domanda di pronuncia pregiudiziale vertente sull'interpretazione e la validità della decisione 2000/520 della Commissione europea del 2000 che constatava che il "*Safe Harbour*" approntato dalla Commissione federale per il commercio degli USA, assicurava un adeguato livello di protezione dei dati personali trasferiti dall'UE. Con sentenza del 6 ottobre 2015, la cd sentenza Schrems I, la CGUE ha dichiarato non valida tale decisione. Successivamente nel 2016, l'UE e gli USA stringevano un nuovo accordo sul trattamento dei dati necessario dopo la decisione *Schrems I*, il cd. "*Privacy Shield*". Questo nuovo accordo doveva fornire un livello di protezione per i dati europeo negli USA almeno equivalente a quello fornito nell'UE. Parallelamente alla decisione della CGUE, l'autorità garante irlandese ha invitato Schrems a riformulare la denuncia sulla base di quanto stabilito nella sentenza *Schrems I*. Questa volta Schrems faceva leva sull'utilizzo eccessivo delle *Standard Contractual Clauses* (SCC) che vincolano il soggetto che tratta i dati a tutelare questi dati in modo conforme a quanto previsto dal GDPR. Secondo Schrems, le SCC non sarebbero state in grado di fornire un'adeguata protezione perché non consentivano un'azione giudiziale idonea allo scopo al proprietario dei dati. Anche questa volta, la CGUE, interpellata dalla suprema corte irlandese, ha invalidato l'accordo tra l'UE e gli USA (*Privacy Shield*) stabilendo che le limitazioni alla protezione dei dati in vigore negli USA non rispettano i principi di adeguatezza e proporzionalità del diritto euro-unitario e che, di conseguenza, i dati europei trasmessi negli USA non sono adeguatamente protetti come avviene invece nell'UE (decisione *Schrems II* del 16 luglio 2020, in: https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX%3A62018CJ0311 [consultato il 15.02.2023]). Questa decisione si applica anche a qualsiasi trasferimento dati al di fuori dello Spazio economico europeo (SEE).

6 Rapporto del Consiglio federale concernente la valutazione della legge sulla protezione dei dati del 9 dicembre 2011, in: FF 2012 227, https://www.fedlex.admin.ch/eli/fga/2012/86/it (consultato il 15.02.2023).

Oltre ad avere approvato la valutazione dell'UFG, il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di esaminare eventuali misure legislative volte a migliorare il livello di protezione dei dati[7], tenendo conto dei risultati della valutazione e delle riforme in corso presso l'UE[8] e il Consiglio d'Europa[9].

Il 29 ottobre 2014, il DFGP ha pubblicato il rapporto esplicativo nel quale ha presentato le sue conclusioni e ha stabilito le linee generali di una nuova legislazione sulla protezione dei dati[10].

Il 1° aprile 2015, il Consiglio federale, avendo preso atto del rapporto del gruppo di accompagnamento, ha incaricato il DFGP di sottoporgli entro la fine di agosto 2016 un avamprogetto di legge per la revisione della LPD orientato alle riforme delle norme sulla protezione dei dati a livello di Consiglio d'Europa e dell'UE, in particolare delle disposizioni del GDPR, della Direttiva UE n. 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nel settore del diritto penale e delle norme sancite dalla Convenzione 108+[11].

Il 21 dicembre 2016, il Consiglio federale ha posto in consultazione l'avamprogetto di revisione totale della LPD e di modifica di altri atti normativi sulla protezione dei dati accompagnato dal suo rapporto esplicativo. La sintesi dei risultati della consultazione è stata pubblicata in data 10 agosto 2017[12].

Il 15 settembre 2017, il Consiglio federale ha licenziato il messaggio relativo alla revisione totale della LPD[13], aprendo in questo modo la via alle delibere parlamentari.

Il processo democratico è stato lungo ed intenso. Il Parlamento ha suddiviso il progetto del Consiglio federale in due tappe distinte: da una parte la trasposizione della Direttiva UE n. 2016/680 sopra menzionata che costituisce uno sviluppo dell'*acquis* di Schengen[14] e, da un'altra, la discussione relativa alla revisione totale della LPD[15].

---

7 Secondo il Consiglio federale, le misure legislative da adottare devono avere come obiettivi di garantire la protezione dei dati sin dalla progettazione del trattamento; di sensibilizzare le persone interessate ai rischi per la protezione della personalità derivante dal progresso tecnologico; di migliorare la trasparenza dei trattamenti dei dati e di rinforzare il controllo e il dominio dei dati già comunicati; di proteggere i minori.

8 L'UE stava rivedendo la propria legislazione sulla protezione dei dati ed in particolare elaborava il progetto di due atti normativi: d'una parte il progetto del GDPR e dell'altra parte quello della Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nel settore del diritto penale.

9 Il processo di modernizzazione della Convenzione 108 è già stato iniziato in 2011 dal Consiglio d'Europa.

10 DFGP, Rapporto esplicativo concernente l'avamprogetto di legge federale relativo alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati del 29 ottobre 2014, Berna, 21 dicembre 2016, in: https://www.bj.admin.ch/dam/bj/it/data/staat/gesetzgebung/datenschutzstaerkung/vn-ber-i.pdf.download.pdf/vn-ber-i.pdf (consultato il 15.02.2023).

11 Tra le novità recepite dalla Convenzione 108+ si segnalano: maggiori tutele per i trattamenti di dati genetici e biometrici, *accountability* del titolare del trattamento, notifica del *data breach*, trasparenza del trattamento, maggiori diritti per l'interessato tra cui quello di non essere sottoposto ad un trattamento automatizzato, valutazione dei rischi connessi al trattamento, *privacy by design*, garanzie per il trasferimento dati in Paesi non aderenti e maggior poteri e attività *awareness* riconosciuti in capo alle autorità di controllo.

12 Il testo della sintesi può essere consultato al seguente link: https://www.ejpd.admin.ch/bj/it/home/staat/gesetzgebung/datenschutzstaerkung.html (consultato il 15.02.2023).

13 Messaggio del Consiglio federale 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, n. 17.059, del 15 settembre 2017, in: FF 2017 5939, https://www.fedlex.admin.ch/eli/fga/2017/2057/it (consultato il 15.02.2023) (cit.: Messaggio nLPD).

14 Il Consiglio federale ha fissato al 1° marzo 2019 l'entrata in vigore delle norme a protezione dei dati nella cooperazione Schengen in materia penale. Si veda la Legge federale sulla protezione dei dati personali nell'ambito dell'applicazione dell'acquis di Schengen in materia penale (LPDS; RS 235.3).

15 Le discussioni in seno alle Camere federali sono iniziate soltanto nel mese di settembre 2019.

Le divergenze delle Camere federali riguardanti, in particolare, la nozione di profilazione si sono finalmente concluse in data 24 settembre 2020 ed il testo finale della revisione totale della LPD è stato accettato dall'Assemblea federale il 25 settembre 2020.

Nel frattempo, la Svizzera ha sottoscritto, in data 21 novembre 2019[16], la Convenzione 108+ e dovrebbe ratificarla con l'entrata in vigore della nLPD.

Il 23 giugno 2021, il Consiglio federale ha avviato la procedura di consultazione sulla revisione totale dell'Ordinanza relativa alla legge federale sulla protezione dei dati (OLPD; RS 235.11) e il 31 agosto 2022 ha fissato al 1° settembre 2023 l'entrata in vigore della nLPD e delle sue disposizioni attuative, nonché la nuova OLPD e la nuova Ordinanza sulle certificazioni in materia di protezione dei dati (OCPD; RS 235.13).

Il presente contributo si soffermerà soltanto su alcuni dei principali nuovi aspetti della normativa. Pertanto, per ogni ulteriore dettaglio, si suggerisce di consultate direttamente il testo della nLPD[17].

III. I principali aspetti della normativa

Anche se ci si trova di fronte ad una revisione totale della LPD, alcune disposizioni rimangono invariate. Infatti, la nLPD continuerà ad applicarsi ai trattamenti dei dati personali effettuati sia dai privati che dagli organi federali (art. 2 cpv. 1 lett. *a* e *b* nLPD).

I principi di base del trattamento sanciti dall'aLPD sono stati comunque ripresi dalla nLPD (artt. 4 e 5 aLPD e art. 6 nLPD). Per quanto riguarda i privati, rimane valido il concetto svizzero di presunzione di liceità del trattamento dei dati personali (art. 30 cpv1 nLPD). Il motivo giustificativo (art. 31 cpv. 1 nLPD), diversamente dal GDPR, sussiste solo in presenza di un trattamento illecito, ossia che rappresenta una lesione della personalità. La violazione dei principi di trattamento, l'opposizione espressa della persona interessata e la comunicazione a terzi di dati personali degni di particolare protezione, rappresentano dei casi di illeceità del trattamento[18]. Invece per quanto riguarda gli organi federali, così come per il GDPR, il trattamento dei dati personali è lecito solo se previsto da una base legale (art. 34 nLPD).

Continueranno a non rientrare nel campo di applicazione della nLPD i dati anonimizzati[19], così come la nLPD non si applicherà ai dati personali ad uso esclusivamente privato (art. 2 cpv. 2 lett. *a* nLPD). A tale riguardo è utile menzionare la sentenza TF n. 5C_15/2001, del 16 agosto 2001, in cui è stata concessa ad un impiegato dell'Università di Ginevra la restituzione dei suoi dati personali e, in particolare, quelli raccolti nell'ambito di una perizia effettuata da uno psicologo su mandato professionale e, pertanto, non ad uso esclusivamente personale.

---

16 Lo stato delle firme e delle ratifiche della Convenzione 108+ sono disponibili al seguente link: https://www.coe.int/it/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (consultato il 15.02.2023). Il Protocollo entrerà in vigore l'11 ottobre 2023 a condizione che entro tale data almeno 38 Stati parte vi aderiranno.

17 Il testo della nLPD è disponibile al seguente link: https://www.fedlex.admin.ch/eli/fga/2020/1998/it (consultato il 15.02.2023).

18 Il motivo giustificativo viene richiesto solo nel caso in cui i principi di trattamento (artt. 6 e 8 nLPD) non vengono rispettati, se la persona interessate si è espressamente opposta al trattamento (art. 30 cpv. 2 lett. *b* nLPD) o se i dati personali degni di particolare protezione sono stati trasmessi a terzi (art. 30 cpv. 2 lett. *c* nLPD).

19 Messaggio nLPD (nota 13), p. 6011. La legge non si applica ai dati che sono stati resi anonimi e la cui identificazione da parte di un terzo è impossibile (i dati sono stati anonimizzati in modo completo e definitivo) o sarebbe possibile soltanto con uno sforzo che nessun interessato è disposto a fare.

In merito alle principali novità, si è deciso di illustrarle in maniera sintetica nella sottostante tabella sinottica aLPD e nLPD a confronto:

Tabella 1: Tabella sinottica aLPD e nLPD a confronto

Tema	**aLPD**	**nLPD**
Campo di applicazione	Persone fisiche e giuridiche (art. 2)	Solo persone fisiche (art. 2)[20]
Sicurezza	Nessuno *standard* minimo (art. 7)	*Standard* minimi di sicurezza (art. 8)
Incaricato federale per la protezione dei dati e trasparenza (IFPDT)	Poteri limitati (artt. 27-33): • no multe/decisioni • emette raccomandazioni a privati • può deferire al Tribunale amministrativo federale	Poteri estesi (artt. 56-58): • inchieste • decisioni vincolanti • comminatoria penale in caso di inadempienza
Dati degni di particolare protezione	Opinioni (religiose, filosofiche, politiche, sindacali), salute, sfera intima, razza, assistenza sociale, provvedimenti o sanzione amministrative/penali (art. 3)	Aggiunta di: • dati genetici • dati biometrici (che identificano in modo univoco una persona) (art. 5)
Notifica delle collezioni di dati	Obbligatorio (art. 11)	Non esiste più
Obbligo di informazione	Solo per dati degni di particolare protezione (art. 14)	Esteso a tutti i dati personali (salvo eccezioni) (art. 19)
Valutazione d'impatto sotto l'acronimo DPIA	Non prevista	Obbligatoria con rischio elevato per la personalità (art. 22)
Notifica e comunicazione *data breach*	Non previsto dalla LPD (solamente nel settore finanziario)	Obbligatorio con rischio elevato e per proteggere l'interessato (art. 24)
Registro dei trattamenti	Non esiste un vero obbligo generalizzato. Esistono solo situazioni in cui bisogna farlo	Obbligo generalizzato (art. 12)
Privacy by design – Privacy by defalut	Prevista ma non in maniera espressa	Introduzione di questi principi in maniere espressa (art. 7)
Profilazione	Abrogata la nozione di profilo della personalità[21]	Adozione della terminologia europea di profilazione[22]
Profilazione a rischio elevato[23]	Non prevista	Profilazione che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata poiché comporta un collegamento tra dati che permette di valutare aspetti essenziali della personalità della persona fisica (art. 5 lett. *g*)

Poiché la nozione di profilazione ha suscitato diversi dibattiti in seno alle Camere federali, è opportuno indicare che la differenza tra i due tipi di profilazione ha una portata limitata[24]. In pratica, le disposizioni della nLPD concernenti i trattamenti dei dati personali effettuati da privati fanno soltanto riferimento alla nozione di profilazione a rischio elevato (ad es. art. 6 cpv. 7 lett. *b* nLPD, art. 31 cpv. 2 lett. *c* nLPD), a differenza dei trattamenti effettuati da parte dagli organi federali per i

[20] Le persone giuridiche, così come per altro le persone fisiche, potranno sempre prevalersi delle disposizioni dell'art. 28 del Codice civile (CC; RS 210) per la protezione dei loro dati personali.

[21] La nozione di profilo della personalità è una particolarità svizzera e corrisponde al risultato di un processo di trattamento ed è quindi ad un dato statico.

[22] La nozione di profilazione indica una determinata forma di trattamento e quindi ad processo dinamico. Inoltre, essa mira ad un determinato scopo il cui criterio determinante è la presenza di un processo di valutazione automatizzato. Una semplice raccolta dei dati non analizzati non costituisce una profilazione.

[23] Nozione assente nel Messaggio nLPD (nota 13) in quanto creata durante i dibattiti parlamentari.

[24] DAVID ROSENTHAL, Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, in: Jusletter 20 febbraio 2017, nm. 28.

quali la nLPD si riferisce alla nozione di profilazione (ad es. art. 6 cpv. 7 lett. *c* nLPD, art. 34 cpv. 2 lett. *b* nLPD).

Come si evince dalla Tabella 1, la revisione più importante della nLPD riguarda l'implementazione delle disposizioni della Convenzione 108+ volte a stabilire una seria di obblighi ai quali i titolari del trattamento devono conformarsi con i principali obiettivi di migliorare la trasparenza dei trattamenti dei dati personali nei confronti delle persone interessate, nonché di rilevare per tempo i rischi per la personalità e i diritti fondamentali delle persone interessate.

IV. Gli obblighi del titolare del trattamento

A. L'obbligo di informare

Una maggiore trasparenza del trattamento dei dati si traduce in obblighi di informazione per il titolare del trattamento e un maggior controllo da parte delle persone interessate sul trattamento dei loro dati rinforzando, di conseguenza, i loro diritti.

Il principio di trasparenza è uno dei principi cardine secondo la LPD che era in vari casi limitato alla riconoscibilità della finalità del trattamento da parte della persona interessata[25]. Questo principio viene ripreso indirettamente dalla nLPD, secondo la quale i dati personali possono essere raccolti soltanto per uno scopo determinato e riconoscibile per la persona interessata (art. 6 cpv. 3 nLPD). Ciò implica che sia la raccolta dei dati che le finalità del trattamento devono essere riconoscibili. La riconoscibilità viene considerata quando s'informa la persona interessata, quando il trattamento è previsto dalla legge o quando lo si evince chiaramente dalle circostanze[26].

I dati personali devono essere trattati in modo compatibile con le finalità iniziali, vale a dire che un ulteriore trattamento non è ammissibile se la persona interessata può legittimamente considerarlo inatteso, inappropriato o contestabile[27].

Il principio di "trasparenza" viene rafforzato dalle nuove disposizioni della nLPD che prevedono un obbligo di informare le persone interessate nei seguenti casi: *(i)* in occasione della raccolta (art. 19 nLPD); *(ii)* nel caso di decisione automatizzate (art. 21 nLPD); *(iii)* nel caso di *Data Breach* (art. 24 nLPD).

1. L'obbligo di informare in occasione della raccolta dei dati

Tale obbligo è esteso a tutti i trattamenti e non solo in presenza di un trattamento di dati degni di particolare protezione come previsto dalla previgente LPD. Questo obbligo vale anche nel caso in cui i dati non vengono raccolti presso la persona interessata (art. 19 cpv. 1 nLPD). In quest'ultimo caso, il titolare del trattamento deve fornire le informazioni in merito al trattamento dei suoi dati entro un mese dalla ricezione dei dati o al più tardi al momento della comunicazione dei dati se i dati sono comunicati prima della scadenza del termine di un mese (art. 19 cpv. 1 nLPD). Le informazioni minime da comunicare alle persone interessate sono l'identità e le coordinate di contatto del titolare del trattamento, lo scopo del trattamento ed eventualmente i destinatari o le categorie dei destinatari a cui sono stati comunicati i dati personali (art. 19 cpv. 2 nLPD).

---

[25] Si veda l'art. 4 cpv. 4 della previgente LPD, secondo cui la raccolta dei dati personali e in particolare le finalità del trattamento dovevano essere riconoscibili da parte della persona interessata.

[26] Messaggio nLPD (nota 13), p. 6016

[27] Messaggio nLPD (nota 13), p. 6016; si veda anche, ROSENTHAL (nota 24), nm. 36.

In caso di trasferimento dei dati personali all'estero (ad es. per i servizi *Cloud* sia sul territorio svizzero che al di fuori dal territorio[28]), la persona interessata deve essere informata sullo Stato o sull'organismo internazionale destinatario e, se del caso, sulle garanzie di protezione dei dati personali, o sulla deroga applicabile nel caso concreto (art. 19 cpv. 4 nLPD).

La nLPD non precisa la forma in cui deve essere fornita l'informazione. Il titolare del trattamento deve provvedere affinché la persona interessata possa effettivamente prendere atto dell'informazione in modo facilmente accessibile[29], ma non deve accertarsi che nel caso concreto la si informi effettivamente[30], così come non c'è alcun obbligo di indicare i suoi diritti o la durata del trattamento a differenza del GDPR (art. 13 GDPR).

Il diritto di informare non è tuttavia un diritto assoluto. Infatti, la nLPD prevede tre categorie di eccezioni (art. 20 nLPD): *(i)* quelle generali (art. 20 cpv. 1 nLPD), come ad es. quando il trattamento è previsto dalla legge o quando c'è un obbligo legale di serbare il segreto, *(ii)* quelle limitate alla raccolta indiretta (art. 20 cpv. 2 nLPD) per quando l'obbligo di informazione richiede ad es. sforzi sproporzionati e, infine, *(iii)* quelle particolari (art. 20 cpv. 3 nLPD) che prevedono ad es. la possibilità di rinunciare all'obbligo d'informare sulla base di un bilanciamento di interesse (ad es. l'interesse preponderante di un terzo, ecc.).

2. L'obbligo di informare in presenza di decisioni individuate automatizzate

Questa nuova disposizione si fonda sull'idea che le macchine non devono prendere delle decisioni relative alle persone, almeno quando si tratta di decisioni importanti.

Per decisione individuata automatizzata s'intende una decisione che è basata esclusivamente su un trattamento automatizzato (algoritmo), ovvero senza interventi umani, e che comporta per la persona interessata delle conseguenze giuridiche o che si ripercuote su di lei in modo significativo[31].

La persona interessata di fronte ad una decisione individuata automatizzata ha il diritto di essere informata e dopo avere esposto il suo parere, ha il diritto ad un riesame da parte di una persona fisica.

Anche in questo caso, la nLPD prevede delle eccezioni (art. 21 cpv. 3 nLPD)[32] all'obbligo di informare, come ad es. nell'ambito della conclusione di un contratto con la persona interessata o in presenza di un consenso espresso della persona interessata.

3. L'obbligo di informare nel caso di Data Breach: violazione della sicurezza

Ai sensi della nLPD, c'è violazione della sicurezza dei dati quando la confidenzialità, l'integrità e la disponibilità dei dati personali vengono compromesse in modo accidentale o illecito e ciò porta alla perdita dei dati personali, alla loro cancellazione, distruzione, divulgazione o vengono resi accessibili a persone non autorizzate (art. 5 lett. *h* nLPD)[33]. Il titolare del trattamento o il responsabile del

---

28 Si fa riferimento alla presa di posizione dell'IFPDT del 13 maggio 2022, pubblicata il 13 giugno 2022 in risposta alla SUVA sul suo imminente progetto di esternalizzazione dei dati personali in centri informatici *Cloud* sul territorio elvetico. La presa di posizione è accessibile al seguente link https://www.edoeb.admin.ch/edoeb/it/home/attualita/aktuell_news.html#651478181 (consultato il 15.02.2023).

29 La modalità dell'obbligo di informare è concretizzata all'art. 13 della nuova Ordinanza sulla protezione dei dati (nOPDa; RS 235.11).

30 Messaggio nLPD (nota 13), p. 6039.

31 Messaggio nLPD (nota 13), p. 6045 s.

32 Messaggio nLPD (nota 13), p. 6046 s.

33 ROSENTHAL (nota 24), nm. 161.

trattamento (altra figura della LPD secondo l'art. 9 cpv. 1 nLPD[34]) devono garantire la sicurezza dei dati mediante provvedimenti tecnici e organizzativi appropriati[35]; questi provvedimenti devono permettere di evitare violazioni della sicurezza (art. 8 cpv. 2 nLPD). È compito del Consiglio federale di emanare le disposizioni minime di sicurezza[36].

Nel caso di una violazione della sicurezza, la nLPD introduce due obblighi di notifica:

a) uno all'autorità di controllo al livello federale (IFPDT) in caso di rischio elevato per la personalità o per i diritti fondamentali della persona interessata (art. 24 cpvv. 1-3 nLPD). In questo caso la notifica deve essere fatta quanto prima (art. 24 cpv. 1 nLPD), senza tuttavia un'indicazione temporale determinata a differenza del GDPR che prevede una notifica all'autorità di controllo competente entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 cpv. 1 GDPR);
b) l'altro alla persona interessata se necessario o se richiesto dall'IFPDT. Anche in questo caso la notifica deve essere fatta quanto prima e anche in questo caso sono previste delle eccezioni (art. 24 cpv. 5 nLPD) all'obbligo di notifica, come ad es. nei casi di restrizione del diritto di accesso, se l'informazione è impossibile o richiede un onere sproporzionato o se una comunicazione pubblica sia sufficiente.

Oltre a migliorare la trasparenza del trattamento dei dati nei confronti delle persone interessate, il testo della nuova legge intende aumentare la responsabilizzazione del titolare del trattamento, il cd. "principio di *accountability*", mediante l'implementazione di misure tecniche e organizzative di cui alcune sono riprese di seguito.

B. La responsabilizzazione: accountability del titolare del trattamento

1. Privacy by design e privacy by default

La nLPD introduce i principi di "*privacy by design*" (protezione dei dati sin dalla progettazione) e di "*privacy by default*" (protezione dei dati per impostazione predefinita) (art. 7 nLPD)[37], secondo cui le aziende sono tenute a progettare, sotto il profilo tecnico e amministrativo, i loro sistemi di trattamento dati in modo da conformarli ai principi di cui alla nLPD.

La protezione dei dati sin dalla progettazione prevede ad es. che le aziende impostino le loro applicazioni in modo che i dati vengono cancellati a intervalli regolari o anonimizzati in maniera standardizzata[38]. Al fine di rispettare questa nuova disposizione, il titolare del trattamento, tenuto conto della finalità perseguita, deve circoscrivere il trattamento dei dati personali al minimo indispensabile. Pertanto, la protezione dei dati fin dalla progettazione materializza il principio di proporzionalità (art. 6 cpv. 2 nLPD) e l'approccio basato sul rischio.

La protezione dei dati per impostazione significa che il sistema è impostato in modo da favorire la protezione dei dati, a meno che la persona interessata modifichi le impostazioni[39]. La particolarità

---

34 Il trattamento dei dati può essere affidato a un responsabile del trattamento per contratto o per legge previo il rispetto delle misure imposte al titolare del trattamento e che non ci sia nessuno contratto o obbligo legale di serbare il segreto.
35 Messaggio nLPD (nota 13), p. 6014.
36 L'art. 8 cpv. 3 nLPD e gli artt. 1-3 OPDa contengono le line guide per determinare i provvedimenti da adottare. Gli artt. 4-5 OPDa, che sono le due misure di *accountability* del titolare del trattamento, stabiliscono i requisiti minimi di sicurezza ai sensi dell'art. 8 cpv. 3 nLPD e sono decisivi affinché il diritto svizzero possa garantire un livello di protezione adeguato rispetto a quello dell'UE (UFG, Ordinanza sulla protezione dei dati [OPDa], Rapporto esplicativo, Berna 31 agosto 2022, p. 18).
37 L'obbligo è previsto anche all'art.25 GDPR.
38 Messaggio nLPD (nota 13), p. 6020.
39 Messaggio nLPD (nota 13), p. 6021.

della protezione dei dati per impostazione predefinita è costituita dal potere conferito alla persona interessata (ad es. l'utente) di decidere quanto esporsi lato *privacy* nei confronti del titolare del trattamento. Ad es., un utente di un sito *web* può decidere a quale tipo di trattamento dati vuole essere sottoposto a dipendenza dei servizi che vuole ricevere[40].

2. Il registro delle attività di trattamento

Il titolare e il responsabile del trattamento hanno l'obbligo di mappare i trattamenti dei dati personali effettuati, inserendo in un apposito registro (art. 12 cpv. 1 nLPD), le indicazioni minime seguenti: il nome del titolare, lo scopo del trattamento, le categorie di interessati, i dati trattati e di destinatari, i tempi di conservazione, le misure di sicurezza a tutela del trattamento ed eventuali trasferimenti all'estero.

Il Consiglio federale prevede delle eccezioni dall'obbligo di tenere un registro delle attività di trattamento (art. 12 cpv. 5 nLPD e art. 24 OPDa) per le imprese e altri organismi di diritto privato che al 1° gennaio di un anno impiegano meno di 250 collaboratori, a prescindere dal loro tasso di occupazione, se non sono trattati su vasta scala dati personali degni di particolare protezione (art. 24 lett. *a* OPDa) e se non viene eseguita una profilazione ad alto rischio (art. 24 lett. *b* OPDa)[41]. Anche se la tenuta del registro non rappresenta un obbligo generalizzato, in quanto per alcune imprese avrebbe potuto comportare un onere amministrativo sproporzionato rispetto ai rischi potenziali, non si impedisce alle imprese esonerate di tenere volontariamente il registro delle attività di trattamento. Anzi, il registro è uno strumento utile e semplice per conservare una visione d'insieme sulle attività di trattamento, il che può semplificare anche il rispetto di altri obblighi come quello d'informazione[42] e ricavare, in modo efficiente, le informazioni importanti sulla conformità di un trattamento con i principi della protezione dei dati[43]. Non c'è alcuna esigenza formale, un semplice foglio Excel o Word è accettabile quanto una soluzione informatica sofisticata.

3. La valutazione d'impatto

La nLPD prevede che il titolare del trattamento debba effettuare una valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment* [DPIA]) quando il trattamento può comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata (art. 22 nLPD). La DPIA è lo strumento di compliance per eccellenza, permette di giustificare i trattamenti di dati più sensibili dal punto di vista del rispetto della protezione dei dati.

La DPIA, analogamente a quanto previsto dall'art. 35 GDPR, è un processo volto a descrivere il trattamento, valutarne la necessità e proporzionalità e facilitare la gestione dei rischi elevati per i diritti e la libertà delle persone fisiche derivanti dal trattamento dei loro dati personali. Sulla base di tale valutazione vanno, se del caso, presi i provvedimenti necessari per ridurre tali rischi[44]. In pratica non sono le lesioni della personalità che sono valutate, ma le conseguenze negative che i trattamenti dei dati potrebbero avere con grande probabilità sulle persone interessate[45]. Il Comitato europeo per la protezione dei dati (*European Data Protection Board* [EDPB]) ha emesso una linea guida concernente la DPIA, nonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del GDPR[46]. Il titolare del trattamento può ritenere che quando un trattamento

---

40 Messaggio nLPD (nota 13), p. 6021.
41 UFG (nota 36), p. 47.
42 UFG (nota 36), p. 48.
43 Messaggio nLPD (nota 13), p. 6027.
44 Messaggio nLPD (nota 13), p. 6047.
45 ROSENTHAL (nota 24), nm. 149.
46 Il testo delle linee guida in materia di DPIA è disponibile al seguente link: https://ec.europa.eu/newsroom/article29/items/611236 (consultato il 15.02.2023). Il motivo della competenza

soddisfa anche uno solo dei criteri elencati, tenuto conto delle circostanze del caso, sia necessario una DPIA.

Se dalla DPIA emerge che, nonostante i provvedimenti previsti dal titolare del trattamento, il trattamento comporta un rischio elevato per la personalità o per i diritti fondamentali della persona interessata, il titolare deve previamente consultare l'IFPDT (art. 23 cpv. 1 nLPD). Esso ha due mesi di tempo per comunicare al titolare le sue obbiezioni contro il trattamento previsto. Il termine può essere prorogato di un mese in casi particolari. Se entro tale termine non riceve alcuna comunicazione dall'IFPDT, il titolare può presumere che l'IFPDT non abbia nessuna obiezione e procede al trattamento previsto[47]. La consultazione dell'IFPDT può essere evitata nel caso in cui venga nominato un consulente alla protezione dei dati ai sensi della nLPD (art. 10 nLPD) e che quest'ultimo sia consultato in merito alla DPIA (art. 23 cpv. 4 nLPD)[48]. Una DPIA non è, per contro, richiesta in caso di trattamento effettuato in virtù di un obbligo di legge (art. 22 cpv. 4 nLPD). Il titolare può, inoltre, rinunciare alla DPIA (art. 22 cpv. 5 lett. *a*, *b* e *c* nLPD) se i suoi sistemi, prodotti e servizi beneficiano di una certificazione ai sensi dell'art. 13 nLPD, così come la DPIA non è neppure necessaria se il titolare rispetta un codice di condotta (art. 11 nLPD).

V. Le sanzioni penali

La revisione totale della LPD, oltre a migliorare e rinforzare la trasparenza dei trattamenti nei confronti delle persone interessate, accentuando il senso di responsabilizzazione del titolare o del responsabile del trattamento, prevede, rispetto al diritto vigente, un inasprimento delle disposizioni penali per adeguarsi al diritto euro-unitario. Con le nuove disposizioni, sia i casi di violazioni soggetti a multe (contravvenzione) che l'importo stesso della multa sono stati aumentati. Tuttavia, diversamente dal GDPR che sanziona quasi tutte le violazioni con sanzioni amministrative pecuniarie importanti[49], non tutte le violazioni degli obblighi sanciti dalla nLPD hanno risvolti sanzionatori diretti. Solo le violazioni intenzionali di determinati obblighi vengono sanzionate. Inoltre, sempre diversamente dal GDPR, il diritto svizzero ha optato per la responsabilizzazione delle persone fisiche in quanto sono i detentori del potere decisionale all'interno dell'azienda e saranno loro a dovere sopportare la multa.

A. La violazione degli obblighi di informare, di concedere l'accesso e di collaborare

Sono puniti, a querela di parte con la multa fino a fr. 250'000, i privati che violano gli obblighi di informare illustrati *supra* ai cap. IV.A.1. e cap. IV.A.2. e il diritto di accesso (artt. 25-27 nLPD) fornendo intenzionalmente informazioni inesatte o incomplete o che omettono intenzionalmente di fornire le informazioni ai sensi della nLPD (art. 19 cpvv. 1 e 2; art. 21 cpv. 1 nLPD) (art. 60 nLPD). Sono puniti, inoltre, con multa i privati che forniscono intenzionalmente all'IFPDT false informazioni o rifiutano di collaborare nel quadro di un'inchiesta (art. 49 cpv. 3 nLPD).

B. La violazione degli obblighi di diligenza

Sono tre gli obblighi di diligenza di cui la violazione intenzionale di privati, a querela di parte, è punita con multa fino a fr. 250'000 (art. 61 nLPD):

---

dell'EDPB è la volontà del legislatore di permettere un'uniforme applicazione del GDPR tra i vari Stati membri, fornendo alle autorità di controllo di ogni Stati membri lo strumento per emettere elenchi simili.

47 Messaggio nLPD (nota 13), p. 6051.

48 Messaggio nLPD (nota 13), p. 6051.

49 Ad es., il GDPR infligge delle sanzioni amministrative pecuniarie sino a 20 mio. di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) in caso di violazione dei principi di trattamento dei diritti degli interessati (art. 83 cpv. 5 GDPR).

- la violazione delle disposizioni relative alla comunicazione di dati personali all'estero (art. 16 ss nLPD);
- la violazione di alcune esigenze imposte al responsabile del trattamento (art. 9 cpvv. 1 e 2 nLPD). Ad es., il titolare del trattamento deve in particolare assicurare che il responsabile sia in grado di garantire la sicurezza dei dati (responsabilità del padrone di azienda previsto dall'art. 55 del Codice delle obbligazioni [CO; RS 220]);
- il non rispetto dei requisiti minimi di sicurezza emanati dal Consiglio federale (art. 8 cpv. 3 nLPD) e sanciti dagli artt. 1-5 OPDa.

C. La violazione dell'obbligo del segreto

La nLPD estende l'obbligo di discrezione del previgente art. 35 LPD ad un obbligo generale di discrezione per tutti i professionisti e stabilisce che è punito, a querela di parte, con una multa fino a fr. 250'000, chiunque riveli intenzionalmente dati personali segreti dei quali è venuto a conoscenza nell'esercizio di una professione che richiede la conoscenza di tali dati (art. 62 nLPD). Tale obbligo vale anche per il personale ausiliario e gli stagisti e non si estingue dopo la cessazione del lavoro/formazione.

Il Consiglio federale ha giustificato quest'estensione dell'obbligo di discrezione a qualsiasi tipo di dati personali invocando in particolare la diffusione massiccia degli *smartphone*[50].

D. L'inosservanza di decisione

Il mancato rispetto dei provvedimenti dell'IFPDT o di una decisione delle autorità di ricorso è perseguito d'ufficio e punito con la multa fino a fr. 250'000. Questo vale sia nel caso di inosservanza di una decisione (art. 63 nLPD) che nel caso di rifiuto intenzionale di collaborare o fornendo intenzionalmente informazioni false nel quadro di un'inchiesta (art. 60 cpv. 2 nLPD), come già indicato *supra* al cap. V.A.

In linea di massima sono punibili con una multa solo le persone, ma se la multa applicabile non supera i fr. 50'000 e se l'identificazione degli autori richiede provvedimenti d'inchiesta sproporzionati, è l'azienda che potrà essere punita (art. 64 nLPD), come lo è anche in caso di crimine o delitto commesso che, per carente organizzazione interna, non può essere ascritto ad una persona fisica determinata. In questo caso l'impresa è punita con la multa fino a 5 mio. di fr. (art. 102 del Codice penale [CP; RS 311.0]).

VI. Conclusioni

Con l'entrata in vigore della nLPD, le aziende dovranno sicuramente rivedere non solo le loro attuali direttive sulla protezione dei dati per essere *compliant*, ma avranno anche il dovere di provare, documentare ed illustrare in maniera circostanziata e regolare (cd. "principio di *accountability*") che hanno implementato un processo volto a proteggere la personalità e i diritti fondamentali delle persone fisiche (dipendenti, clienti, fornitori, utenti *online*) i cui dati sono oggetto di trattamento e, in particolare, che:

- i trattamenti dei dati personali avvengono nel rispetto dei principi sanciti dalle normative sulla protezione dei dati. A tale riguardo occorre sottolineare che la nLPD è una legge quadro che

[50] Messaggio nLPD (nota 13), p. 6087; ROSENTHAL (nota 24), nm. 202.

fornisce gli obiettivi ma non è l'unico elemento normativo in ambito di protezione dei dati personali[51];

- le misure tecniche e organizzative implementate siano appropriate a garantire una sicurezza dei dati personali adeguata al rischio.

Anche se la normativa svizzera è meno severa di quella europea, dal punto di vista delle sanzioni applicate[52] e dei poteri conferiti all'IFPDT[53], i titolari del trattamento avranno tutto l'interesse ad applicare spontaneamente le nuove disposizioni perché oltre a dimostrare la loro compliance alla norma, potrebbero, in riferimento al cosiddetto principio degli effetti, ricadere nel campo di applicazione del GDPR[54] o di qualsiasi altra normativa con le relative conseguenze.

Da ultimo, la *compliance* alla nLPD è la dimostrazione del senso di responsabilizzazione del titolare del trattamento che intende rinforzare il rapporto di fiducia con i suoi dipendenti, clienti, utenti online e fornitori, garantendo un trattamento dei loro dati personali nel rispetto della loro personalità e dei loro diritti fondamentali.

Per ulteriori informazioni rivolgersi a Isabel Costa

---

51 Possiamo citare ad es. l'art 26 dell'Ordinanza 3 concernente la legge sul lavoro (OLL 3; RS 822.113) che riguarda il divieto della sorveglianza (ingiustificata e disproporzionata) del comportamento del dipendente sul luogo del lavoro o ancora l'art. 45*c* della Legge sulle telecomunicazioni (LTC; RS 784.10) riguardante i *cookies* e, in particolare, l'informativa (elaborazione e scopo) e la possibilità per l'utente di rifiutare l'elaborazione (*opting out*).

52 Ad es., nessuna sanzione penale in caso di violazione dei principi basi sanciti dall'art. 6 nLPD, così come nessuna sanzione per quanto riguarda i nuovi obblighi di *governance* come il *Data Breach* o la DPIA.

53 L'IFPDT non ha la facoltà di pronunciare sanzioni (art. 65 cpv. 1 nLPD).

54 Il GDPR si applica alle aziende svizzere che offrono beni o prestazioni di servizi nell'UE ed esercitano un monitoraggio del comportamento dell'utente all'interno del territorio.

Isabel Costa
Manager Privacy
Fidinam & Partners SA
isabel.costa@fidinam.ch
T: +41 91 9731362

Fidinam & Partners SA
Via Maggio 1
6900 Lugano
www. fidinam-and-partners.ch