Rivista Semestrale

Gennaio - Giugno 2021

N. 1/2021

Data Protection Law

Diritto delle nuove tecnologie, privacy e protezione dati personali

PRIVACY E PROTEZIONE DATI PERSONALI

DATA PROTECTION LAW

www.dataprotectionlaw.it

Diretta da Elio Errichiello

www.dataprotectionlaw.it

DATA PROTECTION LAW – RIVISTA GIURIDICA

Rivista online non soggetta ad obbligo di registrazione ai sensi dell'art. 3-bis del Decreto Legge 103/2012

DIRETTORE:
Elio Errichiello

COMITATO SCIENTIFICO:
Elio Errichiello, Livia Aulino, Lucrezia D'Avenia, Rosanna Celella, Giulio Riccio.

Sito web: www.dataprotectionlaw.it

Contatti: info@dataprotectionlaw.it

"Data Protection Law" è una rivista elettronica di diritto Open access pubblicata dall'associazione Data Protection Law. La rivista pubblica con cadenza semestrale numeri costituiti da articoli scientifici inediti, saggi, traduzioni di estratti da opere scientifiche significative e di recente pubblicazione o articoli rilevanti per la comunità scientifica, recensioni di libri ed eventi culturali.
I numeri della rivista ospitano contributi scientifici prodotti e sottoposti su invito diretto della redazione.
Tutti i contributi sono sottoposti a doppia blind peer review.

Indice.

D'AVENIA LUCREZIA E VOLPE GENNARO, I trasferimenti di dati personali dall'Europa agli Stati Uniti: dal Safe Harbor alla sentenza Schrmes II.

Pag. 3

TIZIANA DI PALMA, L'Ethical hacking, configurazione giuridica e nuove prospettive.

Pag. 18

CAMILLO LAUDANNA, Norme privacy in rapporto alla lotta all'evasione fiscale.

Pag. 34

GUARINO GAETANO, La mancata nomina del responsabile per la protezione dei dati personali per i soggetti privati.

Pag. 43

LO CHIATTO FRANCESCO, Diritto allo studio, nuove tecnologie per la didattica e privacy.

Pag. 53

I TRASFERIMENTI DI DATI PERSONALI DALL'EUROPA AGLI STATI UNITI: DAL SAFE HARBOR ALLA SENTENZA SCHREMS II

di Lucrezia D'Avenia e Gennaro Volpe

SOMMARIO: 1. I rapporti tra Europa e Stati Uniti in relazione ai trasferimenti di dati personali: il "Safe Harbor" e la sentenza "Schrems I" – 2. La sentenza "Schrems II" e l'invalidazione del "Privacy Shield" – 3. Le conseguenze giuridiche della sentenza "Schrems II" sui trasferimenti di dati personali negli Stati Uniti d'America – 4. Prospettive per il futuro: le raccomandazioni dell'EDPB e le riflessioni politiche.

This paper aims to highlight the complicated relationship between the EU and the United States regarding the transfers of personal data, from the approval of the Safe Harbor agreement in 2000 to the recent decision of invalidation of the Privacy Shield ruled by the EU Court of Justice the 16° July 2020.
The analysis flows over legal and political topics taking into account legal issues, Courts' judgments and subsequent recommendations powered by the European Institutions.

1. I rapporti tra Europa e Stati Uniti in relazione ai trasferimenti di dati personali: il "Safe Harbor" e la sentenza "Schrems I"

Il Regolamento UE 2016/679 (o "General Data Protection Regulation" o "GDPR") disciplina, nel Capo V, i trasferimenti di dati personali verso i Paesi terzi rispetto allo Spazio Economico Europeo (SEE), prevedendo l'adozione di meccanismi di legittimazione ulteriori rispetto ai trasferimenti intra-comunitari. Prima dell'avvento del Regolamento, erano invece l'art. 25 della Direttiva 95/46 e l'art. 44 del D. Lgs. 196/2003 a vietare il trasferimento dei dati fuori dall'Unione Europea ove non venisse garantito

il rispetto delle condizioni determinate dalla Direttiva stessa [1] e non venissero garantiti livelli di sicurezza adeguati.

In un contesto normativo così delineato, la crescente predominanza di trasferimenti di dati personali, originati all'interno dello SEE, verso entità giuridiche aventi sede negli Stati Uniti, unitamente alle marcate differenze in merito alle normative privacy in vigore nei rispettivi ordinamenti, ha reso, fin da subito, necessario un intervento della Commissione Europea[2]. Con decisione del 26 luglio 2000[3], l'organo esecutivo del processo legislativo europeo istituiva un porto sicuro di approdo, al di là dell'Atlantico, per i dati personali dei cittadini europei.

L'accordo - il cd. "*Safe Harbor*" - da un lato, dava la possibilità alle aziende statunitensi, richiedendo l'iscrizione alla cd. "Safe Harbor List", di godere del regime di libera circolazione dei dati, dall'altro, consentiva ai partner europei, tramite un semplice meccanismo di consultazione, di verificare che tali aziende fossero effettivamente inserite nella lista e avessero recepito nella pratica gli accordi[4]. Per ottenere il riconoscimento dell'adeguatezza del livello di trattamento dei dati personali messi in atto, l'azienda statunitense doveva essere in grado di garantire l'avverarsi di determinate condizioni[5].

---

[1] L'art. 25 della Direttiva UE 95/46 statuiva: *"Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate."*

[2] L'intervento della Commissione Europa trova il suo fondamento nel 6° comma dell'art. 25 della Direttiva UE 95/46, in base al quale le veniva conferito il potere di constatare, secondo la procedura di cui all'articolo 31, paragrafo 2 della Direttiva stessa, che un paese terzo garantisse un *"livello di protezione adeguato […], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, […], ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona".*

[3] Decisione della Commissione del 26 luglio 2000 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, pubblicata in Gazzetta Ufficiale delle Comunità europee il 25 agosto 2000.

[4] La Safe Harbor List conteneva i nomi delle aziende USA certificate, unitamente alla tipologia, al settore di appartenenza e alla data di ottenimento e di scadenza della certificazione.

[5] Le condizioni imposte erano le seguenti: aver aderito al patto entrando volontariamente nella lista delle aziende certificate e rinnovando annualmente la certificazione; avere livelli tecnologici e organizzativi di sicurezza adeguati a evitare la distruzione accidentale o illecita, la perdita accidentale o l'alterazione, la diffusione o l'accesso non autorizzato, o qualsiasi altra forma illecita di trattamento dei dati personali come garantito in Europa; essere disponibile a far verificare le proprie operazioni di trattamento dei dati all'esportatore degli stessi o alla persona/organismo da lui delegato.

Tuttavia, quindici anni dopo la sua stipula, l'accordo, con cui il Dipartimento per il Commercio degli Stati Uniti e i Paesi europei avevano fissato le modalità di esportazione e gestione dei dati personali in territorio statunitense, fu messo in discussione da una prima storica decisione di invalidazione, proveniente dalla Corte di Giustizia Europea.[6] Le origini di tale sentenza vanno rinvenute nelle attività poste in essere dal cittadino austriaco Max Schrems, il quale, a seguito delle rivelazioni di Edward Snowden nel celebre "*scandalo Wikileaks*", decise di rivolgersi all'Autorità Garante Irlandese (competente in quanto la sede di Facebook in Unione Europea è ubicata in Irlanda), sostenendo che i programmi di sorveglianza americani violassero il diritto alla riservatezza degli interessati europei. La questione passò dunque alla Corte di Giustizia locale e, infine, alla CGUE, la quale mise nero su bianco come la legislazione statunitense permettesse alle autorità pubbliche di accedere e trattare i dati trasferiti ben al di là delle esigenze di sicurezza nazionale.

Le conseguenze di tale pronuncia non furono di poco conto laddove si consideri che, quando il 6 ottobre del 2015 la CGUE stabilì che l'"US-UE Safe Harbor Framework" non era più valido perché non garantiva adeguatamente la protezione dei dati durante il trasferimento delle informazioni personali dei cittadini europei verso gli Stati Uniti, le aziende americane che sfruttavano detto accordo per eseguire i trattamenti di dati personali di cittadini europei erano circa 5 mila (tra cui Google e Facebook).

La scelta della Corte trova fondamento, innanzitutto, nella previsione di una derogabilità dei principi stabiliti dall'accordo, laddove "*in conformità all'allegato I, quarto comma, della decisione 2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite […]*"[7]. Secondo la Corte, tale deroga, costituendo un'interferenza illegittima nel diritto europeo della protezione dei dati[8], in quanto prevista in modo incondizionato, rendeva possibili "*ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico*

[6] Sentenza della Corte del 6.10.2015 – Causa C-362/14 avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento Maximillian Schrems contro Data Protection Commissioner.

[7] Sentenza Schrems I (C-362/14 - 6 ottobre 2015) – punto 84 pag. 24.

[8] "*In particolare, la predetta decisione non conteneva alcuna spiegazione relativamente all'esistenza di misure legislative interne o di diritto internazionale, mediante le quali gli USA assicurano un livello*

o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti"[9].
La Corte precisò, inoltre, come le autorità nazionali di protezione dei dati godessero del pieno diritto di indagare sulla base di segnalazioni specifiche, per esercitare le loro funzioni di protezione dei diritti degli individui.
In Italia, il Garante Privacy recepì rapidamente la sentenza con il provvedimento del 22 ottobre 2015, in base al quale per trasferire dati oltreoceano le imprese italiane e le multinazionali operanti nel nostro Paese erano chiamate a ricorrere agli ulteriori meccanismi previsti dalla normativa sulla protezione dei dati personali[10].

2. La sentenza Schrems II e l'invalidazione del *"Privacy Shield"*

In seguito alla sentenza del 6 ottobre 2015, il giudice del rinvio annullò la decisione sfavorevole al sig. Schrems, rinviandola al Commissario per la protezione dei dati[11], affinché riaprisse l'indagine.
In tale contesto, il Commissario, constatato che Facebook Ireland continuava a trasferire i dati personali degli utenti europei negli Stati Uniti attraverso il meccanismo delle clausole standard, previsto dall'art. 46, par. 2 lett. c) GDPR, chiese, quindi, al sig. Schrems di riformulare la propria denuncia.
Accogliendo tale invito, il 1° dicembre 2015, il sig. Schrems chiese al Commissario di vietare o sospendere il trasferimento dei suoi dati verso la società statunitense Facebook Inc., denunciando come una decisione della Commissione Europea[12] non po-

di protezione adeguato avverso le illegittime ingerenze di autorità pubbliche USA (punti 83-88), e appositi strumenti giurisdizionali per reagire alle eventuali illegittime ingerenze delle autorità USA (punto 89)", tratto da *La tutela dei dati personali UE a seguito della sentenza Schrems*, Eurojus, 2015.
[9] Sentenza Schrems I (C-362/14 - 6 ottobre 2015) – punto 87 pag. 24
[10] "*A tal riguardo, facciamo riferimento in particolare all'utilizzo di clausole tipo "Binding Corporate Rules": si trattava in sostanza di redigere delle regole interne da applicare all'intera struttura societaria – indipendentemente dal luogo dove si trovano le branch – volte a regolamentare in maniera unificata proprio il trattamento dei dati personali*", tratto da *Protezione dati personali. Dal "Safe Harbor" al "Privacy Shield",* 2018.
[11] La Commissione per la protezione dei dati (DPC) è l'autorità nazionale indipendente in Irlanda, responsabile della difesa del diritto fondamentale delle persone nell'Unione europea (UE) di proteggere i propri dati personali. Di conseguenza, il DPC è l'autorità di controllo irlandese responsabile del monitoraggio dell'applicazione del regolamento generale sulla protezione dei dati (GDPR).
[12] In sostanza il ricorrente poneva in discussione la validità della decisione 2010/87/UE della Commissione Europea, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46 (GU 2010, L 39, pag. 5), come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016 (GU 2016, L 344, pag. 100).

tesse giustificare il trasferimento dei suddetti dati verso gli Stati Uniti, stante la violazione degli articoli 7, 8, e 47[13] della Carta dei Diritti Fondamentali dell'Unione Europea, derivante dalla messa a disposizione dei detti dati personali alle autorità statunitensi, quali la National Security Agency (NSA) e le Federal Bureau of Investigation (FBI), per essere utilizzati nell'ambito di diversi programmi di sorveglianza.

Il Data Protection Commissoner, visto che la nuova denuncia poneva in discussione una decisione della Commissione Europea, decise di rivolgersi all'Alta Corte irlandese (Hight Court), affinché presentasse rinvio pregiudiziale alla Corte di Giustizia dell'Unione Europea (CGUE).

Nel frattempo, tuttavia, su invito del Gruppo di lavoro *ex* art. 29[14] la Commissione EU e il Dipartimento del Commercio degli USA stipularono un nuovo accordo denominato "Privacy Shield" con l'obiettivo di risolvere i summenzionati problemi di inadeguatezza sollevati dalla Corte di Giustizia relativamente al "Safe Harbor". A tal fine vennero introdotti obblighi più severi per le imprese statunitensi che ricevevano dati di cittadini europei e maggiori garanzie di trasparenza per l'accesso a tali dati delle autorità pubbliche USA per finalità legate alla sicurezza nazionale[15]. Allo scopo di tutelare gli interessati da abusi, assicurare la corretta attuazione dell'accordo e garantire negli Stati Uniti un livello di protezione dei dati equivalente a quello europeo venne, inoltre, istituita la figura del "Mediatore dello Scudo". Il 16 luglio 2016, quindi, la Decisione 2016/1250 della Commissione, stabilì l'adeguatezza del sistema di trasferimento dati tra Unione Europea e Stati Uniti detto "Privacy Shield"[16].

---

[13] L'articolo 7 della Carta garantisce ad ogni persona il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. L'articolo 8, paragrafo 1, della Carta, riconosce invece esplicitamente a ogni persona il diritto alla protezione dei dati personali che la riguardano. Infine, l'art. 47 riconosce il diritto ad un ricorso effettivo e ad un giudice imparziale.

[14] Il Working Party art. 29, noto come WP art. 29, era un gruppo di lavoro indipendente che riuniva le autorità di controllo di tutti gli stati membri. Con l'entrata in vigore del Regolamento Eu 2016/679 tale figura è stata sostituita dal Comitato Europeo per la Protezione dei Dati Personali (EDPB), organo europeo a tutti gli effetti che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati personali.

[15] In virtù della Costituzione degli Stati Uniti, il Presidente, in qualità di comandante supremo ha il compito di garantire la sicurezza nazionale. A tal fine egli può indirizzare le attività dell'intelligence statunitense mediante decreti o direttive presidenziali. Attualmente i due strumenti giuridici centrali sono il decreto presidenziale 12333 e la direttiva presidenziale 28. Quanto alla FISA [*Foreign Intelligence Surveillance Act*] l'art. 702 prevede che la FISC [*Foreign Intelligence Surveillance Court]* non autorizzi singole misure di sorveglianza, bensì programmi di sorveglianza (quali PRISM e UPSTREAM).

[16] Il Privacy Shield, ovvero lo "scudo per la privacy" fra UE e USA, è un meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea. In particolare, le società si impegnano a rispettare i principi in esso contenuti e a fornire agli interessati (i.e. ovvero tutti i soggetti i cui dati personali siano stati trasferiti dall'Unione europea) adeguati strumenti di tutela, pena l'eliminazione dalla lista delle società certificate ("Privacy Shield List") da parte

A questo punto, il giudice del rinvio, rilevando di avere non solo il diritto ma anche l'obbligo di esaminare le eventuali modifiche del diritto verificatesi tra la presentazione del ricorso e l'udienza, stabilì di sottoporre al rinvio pregiudiziale anche la questione sull'interpretazione e la validità della decisione di esecuzione (UE) 2016/1250[17] (cd. decisione Privacy Shield) sulla quale in particolar modo ci soffermeremo[18].

La decisione in oggetto, infatti, aveva carattere vincolante per le autorità di controllo che non potevano, quindi, sospendere o vietare un trasferimento verso una società aderente a tale "Scudo", finchè quest'ultimo era valido ed efficace[19].

La Corte di Giustizia esaminò, quindi, la detta decisione per verificarne la compatibilità con i dettami del Regolamento Europeo 2016/679[20], letto alla luce della Carta Europea dei Diritti Fondamentali (ed in particolare degli artt. 7, 8 e 52 della stessa[21]).

Il punto cruciale di tale analisi, che determinò l'invalidazione dello Scudo, fu rappresentato dal principio di proporzionalità, come codificato dall'art. 52 della Carta e come articolato nell'art. 45 paragrafo 2, lettera a) GDPR.

---

del Dipartimento del Commercio statunitense e possibili sanzioni da parte della Federal Trade Commission (Commissione federale per il commercio). La Commissione europea ha ritenuto che il sistema offra un livello adeguato di protezione per i dati personali trasferiti da un soggetto nell'UE a una società stabilita negli Stati Uniti e che, pertanto, lo Shield costituisca una fonte di garanzie giuridiche con riguardo ai trasferimenti di dati in questione. Lo Scudo UE-USA per la privacy era entrato in vigore il 1° agosto del 2016. Lo Scudo era applicabile a tutte le categorie di dati personali trasferiti dall'UE agli USA, compresi informazioni commerciali, dati sanitari o relativi alle risorse umane, purché la società USA destinataria di tali dati abbia autocertificato la propria adesione allo schema. Tratto da Gruppo di lavoro Articolo 29 – *FAQ per gli interessati in Europa* - WP246 del 13 dicembre 2016.

[17] Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy*.

[18] L'altra questione (posta direttamente dal sig. Schrems) relativa alla validità della decisione di approvazione delle clausole standard emesse dalla Commissione Europea, infatti, ebbe un esito ben diverso. La Corte di Giustizia ritenne, infatti che la decisione 2010/87/UE prevedesse meccanismi efficaci che consentivano, in pratica, di garantire il rispetto di un livello di protezione essenzialmente equivalente a quello garantito all'interno dell'UE dal RGPD e che prevedevano la sospensione o il divieto dei trasferimenti di dati personali, fondati su tali clausole, in caso di violazione delle clausole stesse o in caso risulti impossibile garantirne l'osservanza.

[19] *"Per quanto riguarda, infatti, gli effetti vincolanti della decisione «scudo per la privacy», l'articolo 1, paragrafo 1, di tale decisione dispone che, ai fini dell'articolo 45, paragrafo 1, del RGDP, «gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo [Unione europea-Stati Uniti] dall'Unione alle organizzazioni statunitensi». Ai sensi dell'articolo 1, paragrafo 3, della stessa decisione si considera che i dati personali sono trasferiti nell'ambito di siffatto scudo allorché sono trasferiti dall'Unione a organizzazioni stabilite negli Stati Uniti che compaiono nell'elenco degli aderenti a detto scudo tenuto e pubblicato dal Dipartimento del Commercio degli Stati Uniti".* Tratto dalla sentenza Schrems II (C-311/18 - 16 luglio 2020) – punto 155 pag.37.

[20] In seguito all'entrata in vigore (a partire dal 25 maggio 2018) del Regolamento (UE) n. 679/16 ("GDPR") – che ha sostituito la Direttiva 95/46/CE e tutte le normative locali di recepimento – era inevitabile che il giudizio della Corte utilizzasse quale parametro di riferimento la nuova normativa.

[21] Secondo l'articolo 52, paragrafo 1, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni ai diritti e libertà fondamentali solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Per il contenuto degli altri due articoli citati vedi precedente nota 3.

La CGUE rilevò infatti che detta decisione, al pari della precedente decisione 2000/520, sancisse il primato delle esigenze di sicurezza nazionale rispetto ai principi del regime dello scudo, posti a tutela dei diritti fondamentali delle persone i cui dati personali erano trasferiti dall'Unione verso gli Stati Uniti, senza prevedere alcun limite né garanzie di tutela per gli interessati[22].

Ed infatti l'articolo 45, paragrafo 2, lettera a), del GDPR, conformemente al principio espresso dall'art. 47 della Carta dei Diritti UE, esige che, nel valutare l'adeguatezza del livello di protezione offerto da un paese terzo, si verifichi l'esistenza di adeguati mezzi di "ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento".

Sul punto, la stessa Commissione UE, aveva già rilevato alcune mancanze[23], che aveva però ritenuto superabili in vista dell'istituzione del Mediatore dello Scudo.

Ebbene, secondo l'analisi della Corte di Giustizia, invece, "*il meccanismo di mediazione di cui alla decisione «scudo per la privacy» non è idoneo ad ovviare alle limitazioni del diritto a una tutela giurisdizionale un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati*"[24].

Pur se descritto come "*indipendente dalla comunità dell'intelligence statunitense*", infatti, secondo il giudizio della Corte, il Mediatore non era realmente autonomo rispetto al potere esecutivo. Ciò in quanto era nominato dal Segretario di Stato, costituiva parte integrante del Dipartimento di Stato degli Stati Uniti, e soprattutto, non disponeva del potere di adottare decisioni vincolanti nei confronti dei servizi di intelligence, "*né sono previste garanzie giuridiche da cui sarebbe contornato il suddetto impegno e delle quali potrebbero avvalersi gli interessati*[25]".

[22] Tali ingerenze possono derivare dall'accesso, da parte delle autorità pubbliche statunitensi, ai dati personali, trasferiti dall'Unione verso gli Stati Uniti, e dall'utilizzo di tali dati nell'ambito dei programmi di sorveglianza PRISM e UPSTREAM fondati sull'articolo 702 del FISA, nonché sulla base dell'E.O. 12333. Vedi precedente nota 4.

[23] Sull'articolo 702 del FISA e sull'E.O. 12333 la Commissione stessa ha rilevato la totale assenza di un diritto di ricorso effettivo.

[24] Sentenza Schrems II (C-311/18 - 16 luglio 2020) – punto 194 pag. 43.

[25] Sentenza Schrems II (C-311/18 - 16 luglio 2020) – punto 196 pag. 43.

Da tali osservazioni è conseguita, quindi, in data 16 luglio 2020, una pronuncia di invalidità della "Decisione Scudo Privacy" della Commissione europea per incompatibilità con l'articolo 45, paragrafo 1, del GDPR, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali UE[26].

3. Le conseguenze giuridiche della sentenza "Schrems II" sui trasferimenti di dati personali negli Stati Uniti d'America

Le conseguenze della sentenza "Schrems II" sono state dirompenti. In sostanza, da un giorno all'altro e senza alcuna clemenza[27], la Corte di Giustizia ha imposto ai Titolari (e Responsabili) europei di interrompere ogni trasferimento negli USA basato sul Privacy Shield[28].

Al fine di evitare possibili sanzioni e provvedimenti di blocco dei trasferimenti da parte delle Autorità di controllo, quindi, essendo venuta meno la base giuridica costituita da una decisione di adeguatezza della Commissione Europea, gli operatori hanno subito rivolto la propria attenzione agli altri strumenti giuridici previsti dagli artt. 46 e ss. GDPR: le deroghe di cui all'art. 49 GDPR; le Clausole Contrattuali Standard (Standard Contractual Clauses - SCCs) di cui all'art. 46 e 93 GDPR e le Norme Vincolanti di Impresa (Binding Corporate Rules – BCR) di cui all'art. 47 GDPR.

Laddove il trasferimento dei dati negli Stati Uniti possa trovare la propria base giuridica in una delle ipotesi che costituiscono "*deroghe in specifiche situazioni*" a norma dell'art. 49 GDPR[29], *nulla quaestio*. Non vi è dubbio, infatti, leggendo la lettera della norma[30], che le basi giuridiche individuate nell'elenco dalla stessa fornito costitui-

---

[26] "*Ne consegue che l'articolo 1 della decisione «scudo per la privacy» è incompatibile con l'articolo 45, paragrafo 1, del RGPD, letto alla luce degli articoli 7, 8 e 47 della Carta, e che esso è per tale motivo invalido*" - sentenza Schrems II (C-311/18- 16 luglio 2020) – punto 199 pag. 43.

[27] La Corte di Giustizia ha invalidato la decisione sullo scudo per la *privacy* senza preservarne neanche temporaneamente gli effetti. Non è stato quindi previsto alcun "periodo di tolleranza" come precisato dal Comitato europeo per la protezione dei dati personali (EDPB), nelle "*Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*", adottate il 23 luglio 2020, scaricabili sul sito istituzionale dell'EDPB.

[28] Basti pensare che la maggior parte dei colossi del web (Google, Microsoft, Facebook, etc.) e dei fornitori di servizi in ambito ICT (si pensi alle piattaforme di mail marketing, ai cloud services, ai Provider dei servizi mail etc.) hanno sede negli USA e quindi archiviano i dati di titolarità dei propri clienti su server ubicati negli Stati Uniti.

[29] Vedi nota successiva.

[30] Art. 49, par. 1 e 2 GDPR: "1. *In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa,*

scano una scriminante al generale divieto di trasferimento verso un paese terzo in assenza di garanzie adeguate. Sul punto, anche il Comitato Europeo (EDPB) si è espresso con favore, non mancando, tuttavia, di sottolineare come tali deroghe siano del tutto residuali e ribadendo, in ogni caso, la necessità di interpretare le stesse secondo le precisazioni fornite dallo stesso organo europeo all'interno delle Linee Guida n. 2/2018 dedicate al tema[31]. In particolare, l'EDPB ribadisce che, in relazione alla base giuridica costituita dal consenso, lo stesso deve essere "*liberamente espresso*" e non può costituire la condizione necessaria per l'utilizzo del servizio; in merito al contratto, che può coprire soltanto un trasferimento "*occasionale*" e infine, con riguardo all'interesse pubblico, che deve essere riconosciuto come tale dal diritto dell'Unione o dal diritto degli Stati membri[32].

Se, quindi, non vi è alcun dubbio in merito all'applicabilità dell'art. 49 GDPR ai trasferimenti negli Stati Uniti, lo stesso non può dirsi per gli altri citati strumenti giuridici. La stessa Autorità di controllo irlandese, intervenendo con un commento ufficiale sulla sentenza "Schrems II", ha messo in dubbio la legittimità dei trasferimenti effettuati, sulla base delle SCCs (e lo stesso discorso vale anche per le Binding Corporate Rules – BCR), verso gli Stati Uniti, invitando le omologhe Autorità nazionali a raggiungere una posizione comune sulla questione[33].

è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:
a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri".

[31] Si veda Comitato europeo per la protezione dei dati, *Linee-guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679*, adottate il 25 maggio 2018, in *https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_it.pdf.*

[32] Vedi *supra* nota 27

[33] Il Garante per la protezione dei dati personali italiano si è espresso sul punto solo in un secondo momento, quando l'EDPB ha sottoposto a consultazione pubblica degli stakeholders uno schema di provvedimento sul tema. Il 10 novembre 2020, nel corso della sua 41° sessione plenaria, il Comitato europeo per la protezione dei dati ha adottato, infatti, "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted*", di cui meglio si dirà nel prossimo paragrafo.

Raccogliendo tale invito, quindi, come anticipato, il Comitato Europeo dei Garanti (EDPB) è intervenuto pubblicando sul proprio sito le "*Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*" (cd. FAQ sul caso Schrems), con l'intento di fornire chiarimenti e indicazioni pratiche per gli operatori in difficoltà.

Tale lodevole obiettivo, tuttavia, non può dirsi conseguito. Nelle FAQ, infatti, il Comitato Europeo si limita a precisare che sia le SCCs che le BCR possono fornire una legittima base giuridica per i trasferimenti negli Stati Uniti, soltanto se, ad esito di una valutazione condotta dall'esportatore di dati caso per caso, "*tenendo conto delle circostanze dei trasferimenti e delle misure supplementari eventualmente attuabili*", può concludersi che la normativa statunitense non interferisca con il livello di protezione adeguato dalle stesse garantito[34].

In sostanza, quindi, il Comitato suggerisce agli esportatori di dati di negoziare con l'importatore ulteriori misure di garanzia per gli interessati coinvolti, da inserire nelle SCCs[35] (o nelle BCR). Tale attività dovrebbe, quindi, essere preceduta da una sorta di "*due diligence*" rispetto alle garanzie offerte dal Paese importatore che tenga conto di quanto il singolo importatore sia impattato dalla normativa in oggetto (Sezione 702 FISA e all'E.O. 12333, più volte citate) e del grado di rischio specifico per i diritti degli interessati coinvolti nei trasferimenti (derivante in questo caso dalla possibilità di accesso a tali dati da parte delle autorità governative statunitensi).

In assenza di un provvedimento che individui concretamente le misure supplementari adeguate, gli operatori del settore hanno, quindi, proposto diverse soluzioni. Molte di queste fanno affidamento sulla tecnologia, e, in particolare, sulle tecniche di cifratura e pseudonimizzazione, e più in generale su sistemi che mirano a blindare l'asset di dati trasferito negli Stati Uniti, in modo tale che l'importatore non possa accedervi o che

[34] Vedi Comitato europeo per la protezione dei dati personali, "*Domande più frequenti in merito alla sentenza della Corte di giustizia dell'Unione europea nella causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems*", adottate il 23 luglio 2020, scaricabili sul sito istituzionale dell'EDPB, FAQ n. 5 e 6.

[35] In merito alle SCCs è doveroso segnalare che il 12 novembre 2020, la Commissione Europea ha pubblicato una bozza di decisione contenente nuovi modelli di clausole contrattuali tipo. Tali format, tenendo conto della "decisione Schrems II" prevedono, tra l'altro, disposizioni specifiche relative al rapporto con leggi e autorità degli Stati coinvolti nel processo di esportazione. La bozza può essere consultata sul sito della Commissione al seguente *link*: *Data protection - standard contractual clauses for transferring personal data to non-EU countries (implementing act) (europa.eu)*.

comunque ogni accesso sia tracciato[36]. Altre proposte, invece, mirano ad intensificare gli obblighi di cooperazione dell'importatore, imponendo a quest'ultimo una maggiore trasparenza[37].

4. Prospettive per il futuro: le raccomandazioni dell'EDPB e le riflessioni politiche.

Il 10 novembre 2020, l'EDPB ha reso pubbliche le Raccomandazioni 1/2020[38] e 2/2020[39], mediante le quali il gruppo delle Autorità di Controllo europee ha espresso la propria posizione sulle conseguenze della sentenza "Schrems II", fornendo importanti indicazioni alle aziende su come gestire l'invio di dati personali al di fuori del territorio europeo e, in particolare, verso gli Stati Uniti d'America.
I suddetti documenti si pongono l'obiettivo di aiutare gli esportatori di dati nell'individuazione delle misure supplementari da adottare caso per caso[40] e nella valutazione circa l'adeguatezza normativa dei paesi terzi[41].

---

[36] Sono state proposte, ad esempio soluzioni che propongono l'accesso in remoto tramite credenziali fornite a limitate persone dell'importatore presso i sistemi e i database dell'esportatore. M. MASNADA, Partner, Hogan Lovells Studio Legale, *Schrems II: la sentenza della Corte UE sul Privacy Shield e gli effetti sui trasferimenti extra-UE dei dati personali*, in www.dirittobancario.i, *t*30/07/2020.

[37] Sono state proposte ad esempio clausole aggiuntive che prevedono l'obbligo di notifica preventiva e di autorizzazione dell'esportatore in caso di richiesta di disclosure da parte dell'autorità pubblica straniera ovvero il diritto dell'esportatore di bloccare il flusso di dati e impedire di fatto il trasferimento ulteriore. M. MASNADA, Partner, Hogan Lovells Studio Legale, *Schrems II: la sentenza della Corte UE sul Privacy Shield e gli effetti sui trasferimenti extra-UE dei dati personali*, in www.dirittobancario.it, 30/07/2020.

[38]European Data Protection Board (o Comitato Europeo per la Protezione dei Dati), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, documento pubblicato il 10 novembre 2020 e sottoposto al meccanismo della consultazione pubblica fino al 21 dicembre dello stesso anno.

[39] *Ibidem*.

[40] Come indicato nella sentenza Schrems II, è data la possibilità agli esportatori di dati personali di adottare adeguate misure supplementari che potrebbero colmare le lacune della normativa del paese di destinazione e consentire un livello di protezione sostanzialmente equivalente come richiesto dal diritto dell'UE, tuttavia questa previsione aveva lasciato finora molti interrogativi. N. BERNARDI, *Trasferimento dati personali oltreoceano, si apre uno spiraglio dopo l'invalidazione del Privacy Shield*, in Federprivacy,13/11/2020.

[41] Le raccomandazioni 2/2020 sulle garanzie essenziali europee relativamente alle misure di sorveglianza sono complementari alle raccomandazioni 1/2020 sulle misure supplementari. Le raccomandazioni sulle garanzie essenziali europee forniscono agli esportatori di dati elementi utili a stabilire se il quadro giuridico che disciplina in paesi terzi l'accesso delle autorità pubbliche ai dati per fini di sorveglianza configuri un'ingerenza giustificata nei diritti alla vita privata e alla protezione dei dati personali, e quindi non sia in contrasto con gli impegni assunti dall'esportatore e dall'importatore attraverso lo strumento di trasferimento utilizzato fra quelli di cui all'articolo 46 del RGPD - *Comitato europeo per la protezione dei dati — 41a sessione plenaria: Il Comitato adotta raccomandazioni sulle misure supplementari per i trasferimenti di dati, a seguito della sentenza Schrems II* - European Data Protection Board | (europa.eu).

I soggetti coinvolti, ovvero i Titolari e i Responsabili dei trattamenti che agiscono come esportatori di dati verso Paesi terzi, al fine di effettuare la suddetta valutazione di compatibilità, sono tenuti ad attuare una serie di step prestabiliti.[42]

Il punto di partenza delle attività valutative che competono al data exporter viene cristallizzato dalla Commissione nel censimento completo dei trasferimenti di dati personali effettuati al di fuori dei confini UE, con un occhio particolare al rispetto dei principi di adeguatezza e pertinenza.[43] Trattasi di un adempimento certamente non innovativo, dato che la mappatura dei dati nel registro dei trattamenti rientra già negli obblighi dell'azienda ai sensi dell'art. 30 GDPR, fulcro vitale e punto di partenza di ogni modello organizzativo privacy.[44] Lo stesso discorso, in termini di prevedibilità delle operazioni, può essere mutuato per il secondo passaggio suggerito dall'EDPB, consistente nell'identificazione degli strumenti di trasferimento utilizzati.[45]

L'azienda, che a questo punto avrà mappato i trasferimenti di dati e individuato gli strumenti normativi di legittimazione, si trova ad essere investita di un compito molto arduo: valutare, con la dovuta diligenza e sotto la propria responsabilità, se qualcosa nella legislazione applicabile o nella prassi del paese terzo possa avere un impatto negativo sul livello di protezione dei dati personali.[46] La raccomandazione prevede che in tale operazione il Titolare possa essere assistito dal destinatario del trasferimento.[47]

Se dalla valutazione effettuata il Titolare rileva che lo strumento di trasferimento individuato ai sensi del GDPR non è efficace, allora egli sarà tenuto a considerare, se del

---

[42] European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – punto 6, pag.8.

[43] La Commissione precisa, inoltre, anche l'accesso remoto ai dati da un paese terzo per attività di manutenzione è classificabile come trasferimento, al pari dell'affidamento di dati personali in cloud situati al di fuori dello SEE – punto 13, pag.9 delle Raccomandazioni.

[44] Si veda l'art. 30 del Regolamento UE 2016/679.

[45] Per i trasferimenti verso paesi terzi che hanno ottenuto una decisione di adeguatezza, non sono necessarie ulteriori misure. In mancanza di una decisione di adeguatezza, se il trasferimento è regolare e ripetitivo è invece necessario basarsi su uno degli strumenti previsti dall'articolo 46 GDPR. Per i trasferimenti occasionali, potrebbe essere possibile affidarsi ad una deroga ai sensi dell'art. 49 del Regolamento UE.

[46] Si deve naturalmente trattare di una valutazione effettiva che vada anche oltre il mero dato letterale della legge straniera (un po' come avvenuto nel corso del giudizio Schrems II) osservando l'effettiva compatibilità dell'ordinamento straniero con quelli che sono i principi base del nostro ordinamento […] Purtroppo questo non è sempre facile ma l'EDPB ci viene incontro con un documento […] dal titolo "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*", molto utile per capire quelle che possono essere le garanzie essenziali (riconosciute dall'UE) che uno stato estero o deve garantire, con particolare riferimento ad eventuali diritti di sorveglianza previsti in ordinamenti stranieri (vedi ad esempio quanto previsto dall'ordinamento USA) – tratto da D. DIMALTA *Trasferimento dati extra UE, ecco i consigli pratici di EDPB per risolvere problemi privacy,* in *www.agendadigitale.eu* , 13/11/2020.

[47] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – punto 30, pag.12.

caso in collaborazione con l'importatore, le specifiche misure supplementari di natura contrattuale, tecnica e/o organizzativa, che possano assicurare un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'UE.[48] In assenza di tali misure, il trasferimento non può considerarsi sicuro.

Tuttavia, come è intuibile, se il documento del Comitato Europeo per un verso ha tracciato la via maestra da seguire per i trasferimenti di dati personali verso paesi confinati al di fuori dello SEE, dall'altro non ha concretamente risolto i problemi legati all'invalidazione del "Privacy Shield".

Con la sentenza "Schrems II*",* la Corte di Giustizia dell'Unione Europea ha infatti messo nero su bianco il fatto che le leggi degli Stati Uniti non riconoscono agli interessati un livello di tutela equivalente rispetto a quello loro riconosciuto dalla disciplina europea in materia di protezione di dati personali. Ed è la stessa Autorità Garante per la Protezione dei Dati italiana, attraverso l'autorevole voce dell'Avv. Guido Scorza, a fornire un'interpretazione lucida e disillusa in merito a tale problematica. Mutuando in pieno il pensiero dell'Avv. Scorza, si può affermare, in definitiva, che il problema venutosi a creare non può essere in alcun modo integralmente risolto dal basso, né dall'esterno. Non c'è nessun provvedimento che possa essere adottato dall' EDPB, né da nessuna altra Autorità nazionale di protezione dei dati personali, né, a maggior ragione, nessuna iniziativa contrattuale, organizzativa o tecnologica adottabile da parte di soggetti privati che possa sgretolare il muro eretto dalla Sentenza dei giudici del Lussemburgo e garantire una prosecuzione generale, serena e ininterrotta dei dati personali tra i due continenti. Un problema di disallineamento tra due Ordinamenti si risolve solo intervenendo su uno o entrambi gli ordinamenti[49]. Ciò che servirebbe, in estrema sintesi, è un intervento legislativo che risulti idoneo a ristabilire l'equilibrio perduto.

Uno spiraglio in tal senso potrebbe scorgersi dal cambio di presidenza avvenuto alla Casa Bianca, dove il repubblicano Trump ha lasciato il posto al democratico Biden, alimentando nell'opinione pubblica nuove aspettative circa la possibilità di stabilire

[48] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data – per maggiori dettagli si rinvia al contenuto del paragrafo 2.4 e agli esempi elencati nell'Annex 2.

[49] Intervento di G. SCORZA (Garante Privacy), *Trasferimento dati extra-Ue: "Abbiamo un problema, anzi tre"* , in *www.agendadigitale.eu*, 17/11/2020.

regole forti di tutela in merito alla privacy dei cittadini statunitensi.[50] In questa prospettiva, lo sviluppo di una normativa federale unitaria, che miri alla tutela dei dati personali assicurando tutte le tutele ad oggi previste dalla normativa comunitaria, costituirebbe senza dubbio il primo e decisivo passo da attuare[51], seguito poi dall'istituzione di un'Autorità indipendente dedicata esclusivamente alla protezione dei dati personali.[52] Tutto ciò, va detto, potrebbe anche rilevarsi non sufficiente. Quello che è stato messo in discussione dalla sentenza "Schrems II", di fatto, è principalmente il potere concesso alle agenzie di sicurezza statunitensi, nell'ambito di alcuni programmi di sorveglianza[53], di "spiare" all'interno della vita privata degli interessati, non riconoscendo loro la possibilità di azionare dinanzi ai giudici alcun diritto di ricorso effettivo.[54]

Volendo, infine, allargare il punto di osservazione su una prospettiva globale, un notevole impatto sulla protezione dei dati personali degli interessati potrebbe scaturire anche dai rapporti che gli Stati Uniti e l'Europa decideranno di intrattenere con i Paesi dell'area asiatica. A tal proposito, anche la Cina ha recentemente avanzato un progetto di legge sulla privacy che dichiara di ispirarsi ai principi del GDPR[55]. È dunque possibile che in un prossimo futuro si progredisca verso normative sempre più unitarie, di derivazione europeista, che garantiscano il diritto alla protezione dei dati personali di

---

[50] È questo il pensiero del ministro tedesco dell'economia, Peter Altmaier.

[51] L' "U.S. Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act o Safe Data Act", proposto al Congresso nel settembre 2020, rappresenta la più recente fase dell'evoluzione della legislazione federale sulla privacy. Il Safe Data Act è una versione aggiornata della bozza del testo United States Consumer Data Privacy Act del 2019, che già includeva alcuni obblighi per le aziende, tra cui: ottenere un consenso esplicito per trattare e trasferire dati sensibili; pubblicare delle privacy policy chiare, con l'obiettivo di incrementare la trasparenza nei confronti dei consumatori; porre in essere valutazioni di impatto sulle attività di trattamento ad alto rischio; ridurre al minimo la quantità di dati raccolti, trattati e conservati; adottare politiche non-discriminatorie, per evitare che siano negati beni o servizi a coloro che esercitano i loro diritti. Se emanato, il Safe Data Act attribuirebbe agli interessati diritti di accesso, rettifica, cancellazione e portabilità, imporrebbe la designazione di responsabili della privacy e della sicurezza dei dati e la predisposizione di valutazioni annuali di impatto sulla privacy. Il Safe Data Act estende la definizione di dati "non identificabili", introduce apposite sezioni dedicate alla filter bubble transparency, agli algorithm ranking system e connected device derivati dal Filter Bubble Transparency Act. Ampio spazio è dedicato anche alle pratiche commerciali sleali e ingannevoli. Dal DETOUR Act, il Safe Data Act deriva la disciplina dei dark patterns e manipulation of user interfaces e proibisce alle società di ottenere il consenso o i dati degli utenti attraverso interfacce che oscurano o alterano il processo decisionale o la libera scelta dell'utente – tratto da intervento di G. SCORZA (Garante Privacy), *Trasferimento dati extra-Ue: "Abbiamo un problema, anzi tre"* , in *www.agendadigitale.eu*, 17/11/2020.

[52] *Privacy And Digital Rights For All, A blueprint for the next Administration,* in *https://www.citizen.org/article/public-citizen-transition-memos-a-blueprint-for-the-next-administration.*

[53] Vedi *supra* paragrafo 2 e note 15, 22 e 23.

54 L'esistenza di diritti effettivi e azionabili da parte delle persone i cui dati sono trasferiti è un rilevante criterio di cui deve tenere conto la Commissione europea nella valutazione di adeguatezza del livello di protezione garantito dal paese terzo.

[55] La "*Personal Information Protection Law*", che si appresta ad essere la prima legge organica e sistematica relativa alla protezione dei dati personali, è attualmente in fase di consultazione pubblica.

tutti i cittadini del Mondo? La speranza, all'apparenza utopistica, potrebbe non essere, in fondo, del tutto irrealizzabile.

L'ETHICAL HACKING, CONFIGURAZIONE GIURIDICA E NUOVE PROSPETTIVE

di Tiziana Di Palma

SOMMARIO: 1. I *Computer Crimes*, brevi cenni e la configurazione di nuovi reati – 2. La condivisione universale delle informazioni e le condotte rilevanti ex art. 615-*ter* c.p. – 3. La difficoltà della sanzione per l'accesso "abusivo" ad un sistema informatico e la possibilità dell'*hacking* benevolo.

According to main theme developed by hackers, "information wants to be free", but at the same time, information is needed to examine the process to research legal principles.
In Italy, in 1993, later than other Countries around the World, Italian legislation developed the act n. 547, with the wide purpose to introduce new characters of crimes.
These characters wanted to punish a sort of wrong use of web by a computer user and, especially, the intrusions into private devices.
It's important to note that many computer-users, thanks to their specific skills, could be allowed in their "intrusions", by companies, societies and organizations, to protect from unauthorized access or accidental disclosure to unwanted and unwelcome individuals.
This aspect could be treated as a right access in despite of legal formulation that punishes just the access into an external Informatic system.
Thanks to ultimate jurisprudencial approaches, hackers can't be always defined as enemies.

1. I Computer Crimes, brevi cenni e la configurazione di nuovi reati

Lo sviluppo di nuove tecnologie nel campo informatico e l'utilizzazione sempre più estesa di impianti di elaborazione e trasmissione elettronica di dati hanno determinato l'insorgenza di nuove figure di illeciti che hanno assunto, convenzionalmente, la denominazione di "*Computer Crimes*".

Sul punto, nei lavori preparatori alla legge 23.12.1993 n. 547 (n. 2773), è dato leggere: *"L'uso dei sistemi informatici e telematici ha pervaso le principali attività che vengono svolte nella società moderna, ed una serie sempre più ampia di indicatori lascia prevedere un impatto della risorsa tecnologica più forte e condizionante (...). Fortemente dipendenti dalle tecnologie informatiche appaiono, in particolare, taluni settori di rilevante interesse nell'economia nazionale: quello assicurativo, del credito e delle finanze, industriale, della pubblica amministrazione, del trasporto aereo, ferroviario, metropolitano e marittimo, della sanità e dell'ambiente*".

Fin dagli anni Ottanta del Novecento è stata, quindi, avvertita la necessità di regolare comportamenti potenzialmente dannosi e pericolosi legati alle nuove tecnologie, sì da introdurre in numerosi Stati (in Europa, Danimarca, Norvegia, Austria, Francia, nei Paesi extraeuropei, USA, Canada, Australia, Giappone) una specifica legislazione penale.

Si pensi, a titolo esemplificativo, al *Counterfeit Access Device* and *Computer Fraud and Abuse*, 1984, poi sostituita dal *Computer Fraud and Abuse Act*, 1986; in Danimarca, Legge del 06.06.1985 n. 229, in Norvegia, la Legge, 12.06.1987, in Grecia la Legge, 30.08.1988 n. 1805; in Gran Bretagna, *Computer Misure Act* del 29.06.1990.

In Italia, dunque, con particolare ritardo, è stata emessa la già nominata L. 23.12.1993 n. 547, recante *Modificazioni ed integrazioni alle norme del codice penale e al Codice di Procedura Penale in tema di criminalità informatica*, preceduta solo da sporadici interventi come la l. 18.05.1978 n. 191, con la quale era stato introdotto nel Codice Penale l'art. 420 c.p. che, nel sanzionare l'attentato ad impianti di pubblica utilità, menzionava espressamente anche gli impianti di elaborazione di dati (norma oggi sostituita dall'art. 2 della l. n. 547), o come la L. 01.04.1981 n. 121 contenente il *"nuovo ordinamento dell'amministrazione della Pubblica Sicurezza",* istitutiva di un Centro di elaborazione dati presso il Ministero dell'Interno e rappresentativa della prima forma di tutela di dati archiviati in un sistema informatico.

Agli anni Novanta, sempre in Italia, risalgono, ancora, la l. 05.07.1991 n. 197 che, al suo art. 12, punisce l'uso indebito di carte di credito, il d.lgs. n. 518/1992 che al suo art. 10 disciplina una serie di condotte riassumibili nella definizione di "*pirateria informatica*", la l. n. 675/1996, in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali e il d.lgs. n. 169/1999, attuazione della dir. 96/9/CE relativa alla tutela giuridica delle banche dati nonché la l. 03.08.1998 n. 269,

recante "*norme contro lo sfruttamento della prostituzione, pornografia, turismo sessuale in danno dei minori, quali nuove forme di riduzione in schiavitù*".

In tema di criminalità informatica, prima dell'entrata in vigore della l. 547/1993, dottrina e giurisprudenza tentavano di ricondurre alle fattispecie tradizionali le nuove fattispecie criminose che riguardavano, tra l'altro, truffe commesse attraverso l'elaboratore o altri meccanismi connessi ai software e al complesso di dati e di informazioni immessi nel sistema informatico.

Ad esempio, per quanto riguarda le truffe, si erano manifestate, inizialmente, condotte che avevano ad oggetto gli allora più diffusi sistemi di elaborazione e trasmissione dei dati, ovverosia i sistemi bancari.

Le condotte più diffuse consistevano nell'alterare il funzionamento dei sistemi di trasferimento elettronici dei fondi e nell'accreditare a sé stessi somme di denaro (tecnica del salame)[56].

In dottrina, tuttavia, in ordine a siffatte condotte, ci si avvedeva che mancavano i caratteri tipici del reato, quali estremi essenziali, come gli artifizi e i raggiri, per indurre una persona in errore e per integrare la "truffa" attraverso la creazione di una falsa apparenza della realtà.

In giurisprudenza, tuttavia, si era inizialmente ritenuto applicabile l'art. 640 c.p. in un caso riguardante l'immissione nell'elaboratore elettronico dell'INPS di dati non veritieri relativi a contributi previdenziali non versati[57], ritenendo che fosse stato perpetrato un inganno ai danni dei dipendenti preposti al controllo del versamento dei contributi.

Per altro verso, in merito ai fatti lesivi dei software - poiché per l'hardware rimanevano sempre ipotizzabili le fattispecie di danneggiamento e/o di furto - si era ritenuto di poter applicare, altresì, le disposizioni penali di cui alla l. n. 633 del 1941, sul diritto d'autore, in particolare dell'art. 171, nonostante i plurimi dubbi e perplessità circa la configurabilità del software come opera dell'ingegno.

---

[56] La cd. *Tattica del salame* costituiva un'antichissima tecnica di negoziazione per manipolare l'avversario. "*Consiste nel gestire la negoziazione normalmente e solo alla fine continuare a chiedere piccole concessioni. Proprio come se tagliassimo il salame a fette finissime e l'altro non si accorgesse che, concessione dopo concessione, si è arrivati a metà*" (cfr. Y. DUZERT, M. SIMIONATO, *Newgoziazione: La neuroscienza della negoziazione*, Milano, 2017).

[57] Cfr. Trib. Roma, 20.06.1984.

Per altri, ancora, si è ritenuto che l'accesso abusivo ad un sistema informatico fosse assimilabile al reato di violazione di domicilio ex art. 614 c.p., mentre per l'intercettazione di comunicazioni informatiche o telematiche, si è sostenuta l'applicabilità della disciplina di cui agli artt. 617 e ss. C.p.

Tali forzature, tuttavia, erano suscettibili di minare il principio di tassatività o di determinatezza i quali assicurano, innanzitutto, la certezza della legge per evitare l'arbitrio del giudice, precludendogli la possibilità di punire i casi non espressamente previsti dalla legge: tanto maggiore è la certezza, tanto minore è il soggettivismo, ideologico o caratteriale del giudice[58].

Con l'introduzione della specifica L. n. 547 è stato, indi, ripristinato il principio già espresso nel diritto romano *nullum crimen, nulla poena sine lege,* motivando il Legislatore ad adeguare la legislazione italiana non solo agli interventi già intrapresi a livello europeo ma anche ad uniformare le normative dei diversi Paesi, al fine di combattere in maniera più incisiva un fenomeno per definizione sovranazionale.

Ai fini dell'intervento normativo italiano in materia, ha assunto, in particolare, un ruolo determinante la Raccomandazione "*sur la criminalité en relation avec l'ordinateur*" adottata dal Comitato dei Ministri del Consiglio d'Europa il 13 settembre 1989 [59], la quale ha offerto una ricognizione completa delle sue diverse manifestazioni ripartendo le diverse forme di abuso dell'informatica in due gruppi, relativi, rispettivamente, alla condotte che gli Stati erano invitati a reprimere senz'altro con sanzione penale (cd. "lista minima") ovvero alle condotte la cui repressione penale era lasciata alla valutazione discrezionale dei singoli Stati, non essendosi ancora registrato un consenso unanime sul tipo di tecnica sanzionatoria più adeguato (cd. "lista facoltativa").

Al fine di evitare la creazione di cosiddetti "*paradisi informatici*", ma soprattutto per la necessità di una stretta collaborazione tra gli ordinamenti nella repressione di un fenomeno criminale, come sopra ricordato, in molte delle sue manifestazioni, a carattere "*transnazionale*", la prefata Raccomandazione del Consiglio d'Europa prescindeva dalla circostanza che i diversi Paesi avessero o meno già provveduto ad introdurre disposizioni apposite in materia.

[58] F. MANTOVANI, *Diritto Penale, Parte Generale*, Padova, 1992, p. 98.
[59] Council of Europe, Recommandation n. R (89).

Con la L. n. 547, il Legislatore ha tipizzato nuove figure criminose, collocandole nel corpo del Codice Penale e aggiornato alcune preesistenti fattispecie, atte ricomprendere le condotte proprie della fenomenologia informatica, in luogo di creare una legge speciale, al fine di arginare la sempre più marcata tendenza alla decodificazione.
Alcune ipotesi, dunque, sono state disciplinate ad hoc e collocate nel tessuto normativo preesistente, come l'art. 615-ter c.p., relativo all'accesso abusivo ad un sistema informatico o telematico, l'art. 635-bis c.p., relativo al danneggiamento di sistemi informatici o telematici, e l'art. 640-ter c.p. relativo alla frode informatica.
Con tali interventi si è tentato di porre in luce l'aspetto più critico rappresentato dalla necessità di assicurare una coerenza tra le norme da introdurre e la nature delle tecnologie da regolare, e della conseguente ulteriore necessità non solo di un adeguato approfondimento preventivo dei fenomeni da regolare, ma altresì di prevedere meccanismi di tempestivo adeguamento della normativa all'evoluzione della prassi tecnologica.

2. La condivisione universale delle informazioni e le condotte rilevanti ex art. 615-ter c.p.

Con particolare riferimento alla criminalità informatica, attuata attraverso l'accesso indebito ad un sistema informatico e/o telematico, è bene soffermarsi, in tale breve disamina, sul rapporto hackers-reati informatici.
Il fenomeno dell'*hack* consisteva in un virtuosismo di qualsiasi tipo rappresentativo di una valida soluzione ad un problema attuale.
Il concetto fu presto riferibile all'informatica perché *hackers* si autodefinirono alcuni brillanti studenti delle università americane del Mit e di Stanford in grado, grazie alle loro intuizioni, di superare i limiti che la tecnologia di volta in volta poneva e contribuire, secondo il loro intento, al suo costante progresso.
Per gli hackers, dunque, l'informazione deve poter circolare liberamente perché un sistema, qualsiasi sistema, possa offrire il massimo delle sue potenzialità ed evolversi.
Nacquero poi gruppi isolati di hackers per poi divenire un vero e proprio fenomeno sociale particolarmente variegato e privo di forme di coordinamento definite, ma eticamente contraddistinto dal principio guida "*information wants to be free"*.
Tuttavia liberare l'informazione e condividerla universalmente in nome di un presunto progresso tecnologico e civile costituiva, tuttavia, un pericolo per tutti coloro che (enti

governativi, istituzioni, imprese pubbliche e private, corporazioni etc.) avevano rimodellato la loro organizzazione secondo i nuovi schemi che l'informatica e la telematica avevano offerto.

L'intera società risultava rivoluzionata con la presenza massiva di *personal computer* nelle abitazioni, di sistemi *client-server* negli uffici, secondo la logica funzionale delle nuove forme di comunicazione.

Accanto a tale pervasività delle nuove tecnologie si collocavano indubbie debolezze comunque presenti nei sistemi informatici.

Da qui l'adozione di strumenti normativi, logici, fisici in grado di proteggere i sistemi informatici e telematici, ma soprattutto l'integrità e la riservatezza dei dati in essi contenuti o con questi trasmessi, dalle nuove forme di aggressione.

Anzi, proprio quando la rete Internet era usata da un numero limitato di persone, i primi utilizzatori, per lo più quali sviluppatori di nuovi software, si trovavano di fronte ad un ambiente aperto a possibilità inesplorate di azione, di interazione e cooperazione.

In tale ambito nasceva, indi, l'etica hacker, cioè la prospettiva che enfatizza e premia la creatività tecnologica e la condivisione delle conoscenze che si intreccia con il modello dello sviluppo del software a sorgente aperta (*open source*), modello nel quale tutti i membri di un progetto software hanno la possibilità di accedere ai programmi sorgente, di proporre e realizzare modifiche ed estensioni degli stessi, e di distribuire i programmi originali, così come le loro modifiche ed estensioni[60].

Ne deriva che la menzione *hacker o hacking* non ha necessariamente connotati negativi o rilevanti ai sensi del codice penale, sebbene il termine hacker sia spesso utilizzato per denotare chi si introduce in sistemi informatici altrui contro la volontà del titolare del sistema (commettendo, dunque, il reato di accesso abusivo a norma dell'art. 615-ter c.p.c), al fine, generalmente, di accedere ad informazioni riservate o di compromettere il funzionamento del sistema.

Si osservi, tuttavia, che la cultura hacker rifiuta recisamente tale accezione in nome del ruolo creativo ed inventivo dell'informatica.

Con specifico riferimento alla patologia dell'*hacking* riferita all'art. 615-ter c.p.c si rammenti che secondo la disposizione de qua "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con*

[60] G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione, corso di informatica giuridica*, III ed., Torino, 2016.

la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore di sistema; se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Si è comunemente ritenuto che la configurazione del reato in questione abbia rappresentato la reazione dell'ordinamento all'imperversante fenomeno degli hackers i quali hanno l'indiscutibile capacità e la conoscenza necessarie per accedere "*abusivamente*" ad un sistema informatico, abbandonando, taluni, l'originaria etica.

La condotta rilevante ai sensi dell'art. 615-ter c.p., dunque, consiste:

a) in un qualsiasi tipo di interferenza, resa comunque possibile dallo sviluppo tecnico, nel programma o nella memoria di apparati informatici o telematici non "*aperti*", ma garantiti da una chiave di ingresso o altro mezzo di protezione, contro la volontà del titolare dello *ius excludendi*.

Generalmente non vi sarà contrapposizione espressa di volontà (pur ipotizzabile) ma un inserimento clandestino o con inganno da cui dovrà indursi – salvo prova contraria – il dissenso del dominus.

Questo potrà emergere da atti o fatti incompatibili con un atteggiamento permissivo, del resto di per sé e di norma escluso dal dato stesso della predisposizione di misure di sicurezza (ad es. parola, numero o frase di accesso)[61] .

Non si trascuri che, per la configurazione del reato, può avere rilievo anche una condotta omissiva da parte di chi avendo goduto in precedenza del diritto o del consenso,

[61] "*Il reato tutela non soltanto il diritto alla riservatezza, ma anche più genericamente lo ius excludendi da quello che è stato definito come "domicilio informatico" del titolare*" (Cass. Pen. 07.11.2000).

continui ad ingerirsi quando quello è venuto meno o questo è stato validamente revocato.

b) l'espressione "abusivamente" di cui alla disposizione normativa introduce una nota di antigiuridicità la cui sfera di efficacia non è agevolmente delimitabile.

c) la consumazione del delitto avviene nel momento dell'introduzione nel sistema, trattandosi di reato istantaneo e, nella seconda ipotesi di condotta omissiva, essa interverrà nel momento in cui il titolare del diritto di esclusione manifesti la volontà espressa di esercitarlo o sia eliminato ogni dubbio su una conforme volontà tacita emergente da atti o fatti significativi.

d) il dolo consiste nella cosciente e volontaria ingerenza nel sistema, conoscendo che esso è protetto da misure di sicurezza, o nella volontà di rimanervi malgrado l'intervenuto dissenso del titolare dello *ius excludendi.*

e) Unitamente a tanto, sono contemplate quattro circostanze aggravanti che rendono il delitto procedibile d'ufficio e trattasi di: 1) di abuso dei poteri o violazione dei doveri da parte del pubblico servizio che commetta il fatto, ovvero dell'intervento di investigatore privato che eserciti, pur senza licenza, la professione, o di un operatore del sistema il quale abusi della sua qualità; 2) dei casi in cui il colpevole "*per commettere il fatto usa violenza sulle cose o alle persone*" ovvero "*è palesemente armato"*; 3) dell'ipotesi che dal fatto derivi "*la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati delle informazioni o dei programmi in esso contenuti*"; 4) delle situazioni nelle quali la fattispecie di cui al primo comma sia posta in essere su "*sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico*" con inasprimento ulteriore di pena se, in tal caso, il fatto sia commesso dai soggetti di cui sopra[62].

Come può ben vedersi, questa norma trova la sua collocazione tra i reati contro l'inviolabilità del domicilio, proprio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Cost. e penalmente tutelato nei suoi aspetti essenziali e tradizionali dagli artt. 614 e 615 c.p.c.[63]

---

[62] F. ANTOLISEI, *Manuale di diritto penale*, vol. 2, p. 247, Milano, 2014

[63] R. BORRUSO, *La tutela del docuumento e dei dati, in* AA.VV., *Profili penali dell'informatica,* Milano, 1994, pp. 28 ss.

Posto che l'accesso cui la norma fa riferimento non è quello "fisico" bensì "elettronico" o "telematico", è pacifico che l'atto di intrusione necessita di talune fasi: 1) la raccolta di informazioni necessarie all'azione; 2) la penetrazione nel computer e la manipolazione dei programmi di sistema, mascherandosi da *system manager*; 3) la disabilitazione dei programmi di gestione delle password degli utenti abilitati; 4) l'inserimento del messaggio che si vuole venga letto, in genere sostituendolo ad un programma di utilità di cui necessita il computer; 5) la distruzione (eventuale) di dati; 6) la cancellazione delle proprie tracce[64].

3. La difficoltà della sanzione per l'accesso "abusivo" ad un sistema informatico e la possibilità dell'hacking benevolo

L'accesso è, invero, un'attività che pur non essendo priva di "fisicità" e/ o di materialità, in quanto produce comunque flussi guidati di correnti elettriche o luminose, non è evidentemente caratterizzata dagli elementi tipici della fattispecie della "*violazione di domicilio*" (artt. 614 e 615 c.p.).

Invero, l'art. 615-ter c.p. sanziona esclusivamente l'accesso "virtuale" all'interno del sistema informatico o telematico, che avviene attraverso apposite apparecchiature (terminali, computers) che costituiscono i "ponti" di ingresso al sistema stesso e che consentono di interagire con i dati e i programmi contenuti[65].

Orbene, l'accesso non autorizzato ad un sistema informatico è suscettibile di arrecare il più delle volte un pregiudizio economico alla vittima (basti pensare ai costi legati alle verifiche e agli accorgimenti necessari per evitare – una volta venuti a conoscenza dell'indebita intrusione all'interno del proprio sistema informatico – attentati al sistema stesso) ma anche inficiare la riservatezza e l'integrità dei dati e dei programmi ivi memorizzati.

A differenza di altre manifestazioni tipiche della criminalità informatica, tuttavia, inizialmente si avvertiva una sorta di riluttanza a raggiungere un consenso unanime sulla necessità di sanzionare penalmente le condotte in questione.

[64] F. BERGELLA, *I veri rischi dei sistemi informativi*, in *Il sole 24 ore*, 09.12.1994.
[65] S. RESTA, *I computer crimes tra informatica e telematica,* Padova, 2000.

A tal proposito, a livello internazionale, infatti, il Consiglio dell'U.E. approvava la decisione-quadro relativa agli attacchi ai sistemi di informazione[66] da cui si ricava la definizione di "*Accesso illecito a sistemi di informazione"* (art. 3) per la quale "*l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso, sia punito come reato qualora sia commesso: 1) nei confronti di una qualsiasi parte di un sistema di informazione sottoposto a misure di sicurezza, o 2) con l'intento di cagionare danni a una persona fisica o giuridica, o 3) con l'intento di procurare un vantaggio economico".*

In particolare, la proposta della Commissione, pur non intendendo negare in alcun modo la rilevanza dell'uso di misure tecniche efficaci per proteggere i sistemi d'informazione, aveva ritenuto innegabile che "*un'alta porzione di utenti si espone agli attacchi in quanto non dispone di una protezione tecnica adeguata o addirittura non dispone di alcuna protezione*".

Per scoraggiare, quindi, gli attacchi contro tali utenti, si era ritenuto che l'accesso illecito dovesse essere perseguito non solo nel caso in cui i sistemi disponessero di una protezione, ma anche laddove sussistesse l'intenzione di cagionare un danno o di procurare un vantaggio economico e, così, il Consiglio d'Europa perveniva ad approvare il Trattato sul Cybercrime[67], confermando la scelta nel senso di non sanzionare specificamente le suddette condotte.

Nell'ambito del XV Congresso dell'Associazione Internazionale di Diritto Penale (AIDP), tenutosi a Rio de Janeiro nel settembre del 1994, era stata segnalata, tuttavia, la necessità di un ripensamento della figura de qua, così come espressa dalla definizione inserita nella Raccomandazione dello stesso Consiglio D'Europa del 1989, per la quale l'illecito era genericamente individuato nell'accedere, senza esserne autorizzati, ad un sistema o ad una rete informatica violando le misure di sicurezza [68].

Anche nei già citati lavori iniziali della l. n. 547/1993, si prevedeva una resistenza da parte dei vari governi ad affrontare in modo deciso la repressione dell'accesso *sic et simpliciter* ad un sistema informatico, in quanto "*in massima parte il problema ri-*

[66]Decisione-Quadro (approvata dal) Consiglio dell'UE presentata dalla Commissione COM (2002)173 relativa agli attacchi contro i sistemi di informazione, Bruxelles, 19 aprile 2002.
[67] Convention on Cybercrime, Budapest, 23.11.2001.
[68] Council of Europe - Recommandation Nº R (89) 9, *Accès non autorisé: L'accès sans droit à un système ou un réseau informatique par violation des règles de sécurité;* in Riv. Trim. dir. pen. Econ., 1992, p. 378.

guarda l'hacking benevolo, cioè il fatto di colui che penetra in un sistema senza intenzioni nocive o malevoli ed acquisisce informazioni, usando mezzi illegali per guadagnare l'accesso, quali l'uso di password non ottenute lecitamente, l'elusione di sistemi di sicurezza etc."[69]

Secondo tali considerazioni, il reato così configurato andava contemplato alla luce di un reato di pericolo (astratto), la cui soglia di punibilità era arretrata rispetto all'effettiva lesione di beni di natura personale o patrimoniale.

La fattispecie di accesso abusivo ai sistemi informatici, in altri ordinamenti, veniva variamente configurata, rammentandosi, a tal punto, che la legislazione federale americana contempla diverse fattispecie di reato informatico.

Il paragrafo 1030 del titolo 18 *dell'United States Code*, introdotto con il già citato *Counterfeit access Device and Compurter Fraud and Abuse Act* del 1984, prevedeva originariamente due fattispecie di accesso abusivo finalizzato, rispettivamente, all'acquisizione di informazioni riservate in materia di difesa, relazioni internazionali, ecc., ovvero all'acquisizione di informazioni finanziarie di vario tipo.

In seguito alle modifiche apportate dal *Computer Fraud and Abuse Act* del 1986, a tali fattispecie, rimaste in gran parte invariate, si affiancava una fattispecie di "mero" accesso abusivo, avente ad oggetto solo computer "*di interesse federale*".

In Europa, a mo' di esempio, l'art. 7 della legge portoghese sulla criminalità informatica del 17.08.1991 n. 109 punisce *"chiunque senza esserne autorizzato e avendo intenzione di procurare a sé o ad altri un beneficio o un profitto ingiusto, accede in qualsiasi modo ad un sistema o ad una rete informatici"*.

A contrario, nel codice penale svizzero, per l'art. 143-bis, introdotto con la legge federale del 17.06.1994, realizza la condotta criminosa "*chiunque, senza fine di lucro, si introduce indebitamente, per mezzo di un dispositivo di trasmissione dei dati, in un sistema altrui per l'elaborazione di dati specialmente protetto contro ogni suo accesso*".

Si ricordi ancora il codice penale greco che, con l'art. 370C, introdotto con la l. 26-31-08.1988 n. 1805, punisce "*chi di procura l'accesso ai dati (...) senza che vi sia un diritto a riguardo e violando divieti e misure di sicurezza adottate dal legittimo titolare*" e il codice penale olandese, che, al suo art. 138, inserito con la legge 23.12.1992, prevede "*una pena detentiva non superiore a sei mesi o una pena pecuniaria di terza*

[69] L. PICOTTI, *Studi di diritto penale dell'informatica*, Verona, 1992.

categoria" per chi a) ha violato un sistema di protezione, o b) ha ottenuto l'accesso con mezzi tecnologici, con l'aiuto di falsi segnali o di chiavi false o attribuendosi false qualità".

Alla stregua dell'art. 615-ter c.p., *per contra,* il nostro ordinamento sanziona, *in primis*, l'indebita introduzione nel sistema informatico con qualsiasi mezzo realizzata, al fine di ricomprendere sia l'accesso "da lontano", attraverso le vie di telecomunicazione, sia l'intrusione "da vicino", conseguito da chi si trova a diretto contatto con l'elaboratore altrui.

La tutela penale è riservata ai soli sistemi provvisti di "*dispositivi di sicurezza*" contro accessi indesiderati; perché sia repressa anche la condotta di chi, legittimato all'uso dell'elaboratore, non sia anche autorizzato all'accesso di documenti o programmi conservati in particolari settori della memoria interna del sistema, frequente è la previsione dell'introduzione, oltre che al sistema nel suo complesso, anche in una sola sua parte; l'incriminazione in parola è volta a proteggere la "riservatezza dei dati o dei programmi contenuti nel sistema" e ciò poiché, salvi i casi di introduzioni abusive fini a loro stesse, l'accesso è di regola finalizzato all'acquisizione di dati e/o programmi non disponibili altrimenti.

Il reato così descritto oltre ad essere un reato di pericolo astratto, secondo le ricostruzioni operate in dottrina, è anche un reato di danno, in quanto l'intrusione nell'elaboratore altrui realizzerebbe già compiutamente la lesione di quella che può definirsi "privacy informatica" e sarebbe, quindi, punibile anche nella forma solo tentata[70].

L'elaboratore, inoltre, potrebbe o meno contenere dati o programmi di qualsivoglia tipo, ma, ai fini della realizzazione del reato in esame, tale elemento non avrebbe alcun rilievo, non essendo in gioco l'integrità o la riservatezza di questi ultimi, ma solo la tutela, più formale e al tempo stesso più generale e onnicomprensiva, della macchina che può contenerli.

Anche in base all'art. 614 c.p., peraltro, nessuna rilevanza viene attribuita, nella tutela del domicilio, alla circostanza che l'abitazione o il luogo di privata dimora ad essa equiparato siano del tutto privi di arredi, essendo sufficiente al riguardo che si tratti di luoghi destinati, sia pure in via occasionale, alla "*libera esplicazione della personalità umana*".

[70] F. MANTOVANI, *Diritto Penale, parte speciale I Delitti contro la persona*, Padova, 1995, pp. 450 e ss.

Altra dottrina, tuttavia, sottolinea i flebili contorni della nuova dimensione della sfera di riservatezza individuale[71]: è infatti evidente che nonostante il parallelismo, i sistemi informatici cui l'art. 615-ter c.p. si riferisce non possono essere in alcun modo assimilati ai luoghi privati espressamente menzionati dall'art. 614 c.p. (abitazione, luoghi di privata dimora, etc.), in quanto reputati luoghi di effettiva proiezione spaziale della persona[72].

Per altri, dunque, l'art. 615-ter c.p. proteggerebbe l'interesse alla "*indisturbata fruizione del sistema da parte del gestore*" non diversamente da come l'art. 637 c.p., nel reprimere l'ingresso abusivo nel fondo altrui, protegge "*da ogni possibile turbativa la proprietà fondiaria*" [73].

Ma anche tale prospettiva ha suscitato plurime perplessità in quanto l'art. 637 c.p. prevede il mero turbamento della signoria sull'immobile, punito con una blanda pena pecuniaria allorquando il mentovato art. 615-ter c.p. prevede la più gravosa pena della reclusione fino a tre anni che corrisponde a quella comminata dall'art. 614 c.p. in merito alla violazione di domicilio.

Ad ogni modo, la tesi del "*domicilio informatico*", seppur rivisitata, è stata adottata dal collegio di legittimità che, con la sentenza n. 3067 del 4 ottobre 1999 (VI sez.) ha avuto modo di esprimersi nell'ambito di un procedimento di riesame di un provvedimento cautelare relativo ad una persona imputata dei reati di frode informatica (art. 640-ter c.p.) e di accesso abusivo a un sistema informatico (art. 615 ter c.p.).

Nel caso *de quo*, l'imputata aveva generato, servendosi del sistema telefonico di una filiale di Brindisi della Telecom Italia S.p.A., "*un consistente, anomalo traffico telefonico verso l'estero (Oceania e Isole Cook)"*, a beneficio dei titolari delle due utenze estere oggetto di frequenti collegamenti.

A tali soggetti veniva, infatti, versata una parte delle somme pagate - come da convenzione - dalla società di telefonia italiana agli enti gestori della telefonia nei paesi destinatari delle chiamate.

---

[71] CORRIAS LUCENTE, *Relazione: i reati di accesso abusivo e di danneggiamento informatico*, Seminario di Studi, Roma, 15.12.2000; F. MANTOVANI, *Diritto Penale, parte speciale, cit*., p. 428 e ss.

[72] In tal senso, BERGHELLA - BLAIOTTA, *Diritto penale dell'informatica e dei beni giuridici,* in *Riv. Cass. Pen.*, 1995; F. MANTOVANI, *Brevi Note a proposito della nuova legge sulla criminalità informatica*, in *Critica del diritto*, 1994, n. 4.

[73] M. MANTOVANI, *Ingresso abusivo nel fondo altrui,* in *Noviss. Dig. It.* Vol. VIII, 1962, p. 696.

A pronunciarsi sulla questione del bene giuridico tutelato dalla norma sull'accesso abusivo, la Corte è stata indotta dalla circostanza che il Tribunale di Lecce, come Tribunale del riesame, aveva escluso che, nel caso di specie, si fosse verificata una violazione di tale disposizione, non avendo l'imputata ottenuto, con la sua condotta, "*alcuna informazione riservata che potesse ledere la riservatezza individuale dei soggetti che a tali sistemi possono legittimamente accedere*".

Nell'annullare sul punto l'ordinanza cautelare, la Cassazione ha precisato che, delle diverse opinioni emerse in dottrina al riguardo, quella preferibile è nel senso che oggetto della norma in esame sia "*lo ius excludendi del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla propria sfera di pensiero o alla propria attività (lavorativa e non)".*

Secondo una diversa lettura, invece, l'art. 615-ter c.p., nonostante la sua collocazione sistematica, sarebbe finalizzato a proteggere l'integrità dei dati e dei programmi in esso contenuti dal pericolo cui risulterebbe esposta in presenza di un accesso abusivo[74].

Significativa, sul punto, sarebbe la previsione di aumento di pena nel caso in cui "*dal fatto derivi la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti*" (II comma n. 3).

Dirigendo l'attenzione sugli sviluppi giurisprudenziali del tema e, in particolare, su quelli più recenti, si è ritenuto che la fattispecie contemplata ex art. 615-ter c.p., invero, può essere integrata anche da un soggetto che sia "*formalmente abilitato ad accedere al sistema*", anche da parte di un dipendente pubblico, ma che vi si trattenga in contrasto con la volontà dell'avente diritto, contravvenendo alle prescrizioni impartite dal titolare (basti pensare alle disposizioni organizzative interne ad un'azienda, a prassi aziendali) o comunque compiendo operazioni diverse da quelle cui il soggetto era incaricato.

Le Sezioni Unite, con pronuncia del 08.09.2017 n. 41210, sono pervenute ad ampliare la portata del *dictum* sopra richiamato, con specifico riguardo all'ipotesi in cui il delitto sia stato commesso ad opera di un pubblico ufficiale o di un incaricato di un pubblico

[74] M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, *cit.*, p. 18 ss.; nel senso che la norma sia diretta a tutelare anche, e in via eventuale, un interesse patrimoniale, "*relativo al possibile danneggiamento della struttura; come si desume dalla previsione aggravatrice di cui all'art. 615 ter capoverso n. 2*", MARINI, *Delitti contro la persona*, II ed., Torino 1996, p. 385.

servizio, concordando sulla possibilità di ritenere integrato il reato de quo anche laddove "*l'agente, pur essendo abilitato all'accesso e pur non violando le prescrizioni formali impartire dal titolare di un sistema, abbia fatto ingresso o si sia mantenuto al suo interno per ragioni ontologicamente estranee e comunque diverse rispetto alle esigenze di servizio per le quali la facoltà di accesso gli era stata attribuita*".

Non sempre eseguire un accesso ad un sistema informatico *"estraneo*" è, tuttavia, suscettibile di configurare una fattispecie delittuosa e, probabilmente, tale considerazione deriva dalla percezione dell'utilità potenziale proveniente dalle capacità e competenze tecniche hacker.

E sul punto, a mo' di esempio, può citarsi la recentissima pronuncia della Cassazione Penale sez. V, del 02.10.2020 n. 34269, per la quale *"per giudicare della liceità dell'accesso effettuato da chi sia abilitato ad entrare in un sistema informatico occorre riferirsi alla finalità perseguita dall'agente, che deve essere confacente alla ratio sottesa al potere di accesso, il quale mai può essere esercitato in contrasto con gli scopi che sono a base dell'attribuzione del potere, nonché, in contrasto con le regole dettate dal titolare o dall'amministratore del sistema. Tanto vale per i pubblici dipendenti ma, stante l'identità di ratio, anche per i privati, allorché operino in un contesto associativo da cui derivino obblighi e limiti strumentali alla comune fruizione dei dati contenuti nei sistemi informatici. In tal caso la limitazione deriva non già da norme pubblicistiche, che non esistono, ma dai principi della collaborazione associativa, che hanno, come base necessaria, il conferimento di beni, utilità, diritti e quant'altro funzionali al perseguimento dello scopo comune e impongono l'utilizzo degli stessi in conformità allo scopo suddetto. Anche l'accesso ai sistemi informatici predisposti a servizio dell'attività comune deve avvenire, quindi, in conformità alla ratio attributiva del potere, configurandosi come abusivo, ai sensi dell'art. 615 ter, ogni accesso che risulti con esso incompatibile".*

Assai interessante si collocava il caso di un hacker che, attraverso la sua attività di accesso a svariati sistemi informatici e/o telematici, aveva individuato talune fallacità nel sistema dell'azienda cui aveva eseguito l'accesso.

Avendo provveduto infruttuosamente a contattare ed avvisare il titolare dello *ius excludendi alios* dell'errore così individuato, stante la sua inerzia, il soggetto indagato si decideva a notiziare la presenza dell'errore de quo nel sistema, invocando la cd. "*divulgazione responsabile*".

Con il decreto di archiviazione del 15.07.2019, emesso dal g.i.p. presso il Tribunale di Catania, dunque, è stato dato ingresso all'*ethical hacking*, conferendo dignità al concetto di divulgazione responsabile, ritenendo non violato sic et simpliciter il disposto dell'art. 615-ter c.p.c., "*avendo peraltro il soggetto contattato prima l'azienda coinvolta proprio per consentirle di emendare l'errore entro un lasso di tempo*".

Nel caso de quo, pertanto, il Giudicante ha ritenuto l'operatività della scriminante di cui all'art. 51 c.p.c, che contempla il "diritto di critica" tenuto conto della veridicità della notizia diffusa.

A ciò aggiungasi, altresì, la riflessione per la quale la "*divulgazione responsabile*" è finalizzata a prevenire gli attacchi informatici il che ha avuto la valenza di favorire l'incremento di nuove figure professionali specifiche per contrastare le minacce alla *cyber security* aziendale, corrispondenti ai *bug hunter* che non sono altro che hackers etici, alla ricerca, grazie alle competenze tecniche maturate, delle fallacità all'interno dei sistemi informatici (siti web, domini) in capo ad aziende e anche istituzioni che autorizzano le attività di accesso ai predetti sistemi (*pen testing*).

In Italia tale processo è ancora agli albori, segnalandosi, tuttavia, Telecom Italia che, dal 2018, si affida agli hacker per scoprire la eventuale presenza di bug all'interno dei propri sistemi.

NORME PRIVACY IN RAPPORTO ALLA LOTTA ALL'EVASIONE FISCALE

di Camillo Laudanna

SOMMARIO. 1. Premessa. - 2. Legge di Bilancio e interventi del Garante della Privacy. - 3. Problematiche: fattura elettronica, trattamenti automatizzati e interconnessione di banche dati, pseudonimizzazione. - 4. Limiti ai diritti dell'interessato. - 5. Conclusioni.

Considering the new financial law, the use of technological tools by the Revenue Agency and the Financial Guard is certainly an important aspect in the fight against fraud and prevention of tax evasion. Nevertheless, the discipline requires to be in line with the European Data Protection Law. Therefore, today it is important to reflect and understand how much you want to sacrifice your privacy in favor of prevention and contrast of tax evasion.

1. Premessa

Da tempo i rapporti tra Fisco e Garante della Privacy non sono dei migliori. Difatti diversi interventi del Garante in questi ultimi anni hanno evidenziato numerose criticità relative al sistema di acquisizione dei dati da parte dell'Anagrafe Tributaria, alla sicurezza e alla qualità delle informazioni archiviate, alla quantità delle informazioni raccolte (molte delle quali non pertinenti con gli obiettivi prefissati), ai canali di trasmissione definiti poco sicuri e alla conservazione dei dati raccolti.
È questo lo scenario con il quale ci si imbatte quando si parla di lotta all'evasione e tutela della privacy dei cittadini, soprattutto in considerazione del fatto che negli ultimi anni sono sempre più i mezzi, e sempre maggiormente invasivi, messi a disposizione dell'Agenzia delle Entrate per combattere l'evasione, così come sono sempre più anche i profili di rischio legati al trattamento dei dati personali nelle fattispecie considerate.

2. **Legge di bilancio e interventi del Garante della Privacy**

Lungo il dibattito che c'è stato tra mondo politico e Garante per la protezione dei dati personali in merito all'approvazione della nuova legge di bilancio, che però, nonostante i diversi interventi, ha ugualmente visto la luce introducendo novità di particolare rilievo.

Infatti, l'articolo 1 comma 681 ha modificato l'art. 2 sexies del D.Lgs. 196/2003, immettendo nuove fattispecie che classificano tra i trattamenti di dati personali di rilevante interesse pubblico anche quelli relativi all'attività di soggetti pubblici deputati alla prevenzione e al contrasto dell'evasione fiscale. Altra nota amara quella della difficoltà per gli interessati di esercitare in modo effettivo i diritti normalmente garantiti loro dagli articoli 15-22 del GDPR in materia tributaria e nello svolgimento di attività legate alla lotta all'evasione. Alla luce di tali novità era scontato che vi fossero numerosi scontri tra il mondo politico ed il Garante in merito alla nuova legge di bilancio.

Infatti, solo negli ultimi mesi vi sono stati ben quattro interventi[75] del Garante Privacy in cui venivano analizzate le novità introdotte dalla nuova legge e le relative problematiche emergenti in riferimento alla privacy. A seguito delle due memorie[76] del Presidente dell'Autorità Antonello Soro del novembre 2019, ha avuto origine un acceso dibattito col mondo politico che difatti accusava il Garante di ostacolare la lotta all'evasione. L'Autorità Garante, quindi, ancora nella persona del Presidente, ha dovuto rispondere, nell'intervista rilasciata al Sole24Ore[77], dichiarando che l'attività dell'Autorità non tende a limitare l'Agenzia delle Entrate nell'attività di contrasto all'evasione, ma solo a proteggere le informazioni fornendo le più adeguate indicazioni. Il Presidente Soro ha, inoltre, ribadito con forza che non si può pensare che l'Agenzia delle Entrate non sia in grado di svolgere la funzione di elaborazione dei dati e di analisi dei profili di rischio perché il Garante lo impedisce, dichiarando che non c'è alcun dubbio nel considerare la lotta all'evasione di interesse pubblico, ma al

[75] Memoria del Presidente del Garante per la protezione dei dati personali sul disegno di legge C. 2220, di conversione in legge del decreto-legge n. 124 del 2019, recante disposizioni urgenti in materia fiscale e per esigenze indifferibili, 5 novembre 2019.
[76] Memoria del Presidente del Garante per la protezione dei dati personali sul disegno di legge di bilancio 2020,12 novembre 2019.
[77] Antonello CHERCHI, Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali, in "*IlSole24Ore*", 18 novembre 2019.

contempo chiedendo una attenta disamina di tematiche che non erano state correttamente analizzate. Alla luce dei diversi interventi, quindi, sono state evidenziate molte tematiche con numerose criticità, in particolar modo connesse a: pseudonimizzazione, trattamenti automatizzati e interconnessione di banche dati, limitazioni dei diritti dell'interessato e mancata osservazione dei principi di proporzionalità e necessità.

3. Problematiche: fattura elettronica, trattamenti automatizzati e interconnessione di banche dati, pseudonimizzazione

Tra le problematiche più rilevanti senz'altro è da considerare quella relativa alle fatture elettroniche e soprattutto alla conservazione delle stesse. Infatti la nuova normativa prevede che il file .xml contenuto all'interno della fattura elettronica possa essere conservato fino al 31 dicembre dell'ottavo anno successivo a quello di presentazione delle dichiarazioni dei redditi e ad ogni modo fino alla definizione di eventuali giudizi[78]. Inoltre, come già evidenziato in un precedente provvedimento del 2018, la memorizzazione dei dati in oggetto mal si concilia con i principi di necessità e proporzionalità, in considerazione del fatto possono essere conservati anche dati non fiscalmente rilevanti, quali, a mero titolo esemplificativo, informazioni inerenti alla descrizione delle prestazioni fornite. Infatti, spesso, nelle fatture elettroniche vi è un numero di informazioni ben più alto di quello necessario all'Agenzia delle Entrate per combattere l'evasione, quali quantità e qualità dei beni o ancora abitudini di consumo o appartenenza dei clienti a determinate categorie. A tal proposito il Garante[79] ha proposto di oscurare i dati non rilevanti ai fini fiscali, proprio per tutelare maggiormente la privacy del singolo individuo e per evitare di catapultarlo all'interno di una lotta impari con l'Agenzia delle Entrate nella quale il cittadino, da un lato è costretto a condividere i suoi dati nella propria interezza e anche se non strettamente necessari ai fini fiscali, dall'altro, invece, non ha il diritto di conoscere quali dati siano posseduti e utilizzati dall'Autorità Tributaria nell'ambito di un accertamento fiscale. Si noti come sia pro-

[78] L. TUCCI, *Legge di bilancio 2020, lotta all'evasione e rischi privacy alla luce del GDPR,* in Agenda Digitale, *www.agendadigitale.eu*, 2020.
[79] A. FONTANAROSA, *Il Garante: "Dati sulla salute degli italiani al Fisco con il pretesto della lotta agli evasori",* in La Repubblica, *www.repubblica.it*, 2019.

prio questa totale asimmetria tra le due parti ad aver fatto sì che il Garante per la protezione dei dati personali ponesse l'accento sul rispetto del principio di necessità e proporzionalità.

A livello squisitamente tecnico c'è da aggiungere come, in Italia, con il provvedimento 30 aprile 2018 del direttore dell'Agenzia delle Entrate, sono state stabilite le regole tecniche per l'emissione e la ricezione delle fatture elettroniche per le cessioni di beni e le prestazioni di servizi effettuate tra soggetti residenti, stabiliti o identificati nel territorio dello Stato e per le relative variazioni, utilizzando il Sistema di Interscambio. In base a tali regole la fattura elettronica consiste in un file in formato .xml, non contenente macroistruzioni o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. In ambito europeo la situazione è però ben diversa: infatti, nessun altro Stato membro ha adottato la fatturazione elettronica tra privati, a parte l'Italia ed il Portogallo.

C'è, tra l'altro, da aggiungere come il legislatore italiano abbia mostrato una certa consapevolezza dei rischi per i diritti e le libertà degli interessati derivanti dalle nuove disposizioni normative, al punto da prevedere un regime diverso per le prestazioni sanitarie escludendo dall'obbligo di fatturazione elettronica i soggetti che inviano dati al Sistema TS[80] nonché i soggetti che, pur non tenuti all'invio dei dati al Sistema TS, emettono fatture comunque relative a prestazioni sanitarie effettuate nei confronti delle persone fisiche. Inoltre, il legislatore stesso ha disposto che nell'utilizzazione dei file acquisiti dalle fatture elettroniche la Guardia di Finanza e l'Agenzia delle Entrate, sentito il Garante per la protezione dei dati personali, dovranno adottare idonee misure di garanzia, anche di carattere organizzativo, a tutela dei diritti e delle libertà degli interessati, in conformità con le disposizioni del GDPR e del novellato Codice in materia di protezione dei dati personali.

Altra problematica messa in risalto dalla valutazione delle criticità della nuova Legge di bilancio è quella relativa ai trattamenti automatizzati e alla interconnessione di banche dati. Si prevede, infatti, l'utilizzo da parte dell'Agenzia delle Entrate e della Guardia di Finanza delle informazioni contenute nell'archivio dei rapporti finanziari per le attività di selezione ed analisi del rischio di evasione, da effettuarsi attraverso procedure automatizzate ed informatizzate di interconnessione con le altre banche dati

[80] A. CATALETA, G. FAGGIOLI, *Decreto fiscale 2020, i problemi privacy della lotta all'evasione,* in *www.agendadigitale.eu*, 2019.

dell'Anagrafe Tributaria. Infatti, come già detto in precedenza in merito alla fatturazione elettronica, anche in questo caso si rischia di memorizzare una infinita mole di dati.

È fuori dubbio il fatto che utilizzando le ultime tecnologie basate su elaborazioni su larga scala e interconnessione di banche dati si vada a ledere quello che è il principio di minimizzazione così come previsto dal GDPR, e quindi quelle che sono le caratteristiche di adeguatezza, pertinenza e limitatezza del dato raccolto solo in relazione a quanto necessario per le proprie finalità e quindi in questo caso solo limitatamente ai dati fiscali. Sarebbe opportuno, a riguardo, che le elaborazioni di dati su larga scala siano sottoposte sempre ad accurata analisi, anche e soprattutto enfatizzando quella che è la presenza del fattore umano[81] per creare una simbiosi tra quest'ultimo e la tecnologia utilizzata e meglio tutelare i diritti e le libertà degli interessati, senza lasciare alla macchina un'analisi libera e incondizionata. A tal proposito quello che balza agli occhi nella nuova legge di bilancio è la legittimazione a questo utilizzo incondizionato dei trattamenti automatizzati sia da parte della Agenzia delle Entrate che da parte della Guardia di Finanza, con evidenti rischi, così come precisato dal Garante Privacy, di disallineamento o duplicazione delle informazioni, nonché di attenuazione della qualità di dati.

È giusto il caso di precisare come sia evidente che l'art. 86 della legge di bilancio da un lato allarga l'uso delle banche dati fiscali in funzione antievasione, dall'altro, però, restringe quelle che sono le tutele per i dati personali dei contribuenti[82]. Concedendo all'Agenzia delle Entrate e alla Guardia di Finanza di far ricorso all'archivio dei rapporti finanziari nel quale sono custoditi innumerevoli dati riferiti a conti correnti e altri rapporti si rischia di comprimere troppo i diritti dei cittadini. Infatti, nel testo, si legge che le operazioni tese a prevenire e contrastare l'evasione fiscale sono diventate di rilevante interesse pubblico e quindi si va, di fatto, a legittimare l'attività dell'Autorità Tributaria, il cui obiettivo risulterà senza dubbio più facilmente perseguibile attraverso l'interconnessione con le altre banche dati di cui il Fisco dispone, in modo da poter elaborare modelli che consentano di individuare i profili dei contribuenti che non pagano le tasse, andando però, al contempo, ad aggirare la normativa privacy e togliendo

[81] R. D'ELIA, *Lotta all'evasione fiscale VS privacy nella Legge di Bilancio: l'allarme del Garante,* in Informazione fiscale, *www.informazionefiscale.it*, 2019.

[82] R. MOSCIONI, *Privacy, i controlli anti-evasione violano i diritti dei cittadini*, in Edotto, *www.edotto.com*, 2019.

la possibilità ai contribuenti di esercitare i propri diritti. Inoltre è ormai empiricamente provato come l'utilizzo dei dati personali con nuove tecnologie e, addirittura, con dati diversi da quelli presenti nelle banche dati ufficiali, sarà sempre più frequente. Basti pensare che il Fisco, di fatto, va ad analizzare non solo i dati presenti nelle dichiarazioni, nelle fatture elettroniche, negli estratti conti, e quindi negli archivi ufficiali dell'Anagrafe Tributaria, ma anche nella miriade di informazioni presenti sul web e sui social.

Recenti provvedimenti giurisdizionali e circolari dell'Agenzia delle Entrate fanno, infatti, spesso riferimento a dati raccolti online e sono numerosissimi i contribuenti la cui posizione viene analizzata partendo magari da foto pubblicate da loro stessi sui social network. Ciò premesso, occorre tuttavia precisare che nel recente passato sia il Garante della privacy con il provvedimento del 29/4/2019, che la magistratura amministrativa con la sentenza del Consiglio di Stato n. 2270/2019, hanno ulteriormente evidenziato le difficoltà nel caso di utilizzo di algoritmi o funzioni di calcolo automatizzate. Nello specifico entrambi gli organi sopra citati hanno precisato che l'utilizzo di tali tecniche informatiche debba essere esplicitato nelle successive motivazioni degli atti amministrativi in modo che il contribuente, ed eventualmente anche il giudice adito, possano comprendere esattamente il funzionamento degli algoritmi utilizzati. Solo potendo avere contezza dei criteri di selezione che sono stati utilizzati il contribuente potrà infatti tutelare i suoi diritti di fronte al giudice competente. Queste attività di esplicitazione degli algoritmi devono essere svolte in contraddittorio con il contribuente. Queste prescrizioni, compresa la verifica della qualità dei dati e delle informazioni utilizzate dall'algoritmo da parte di un essere umano, devono essere rispettate pena la nullità dell'atto amministrativo conseguente.

Si nota, inoltre, come per le decisioni fondate su trattamenti automatizzati normativamente previsti, venga imposto anche di introdurre misure adeguate a tutela dei diritti e delle libertà degli interessati. Se le analisi del rischio per la prevenzione e il contrasto all'evasione fiscale si affidano ad un algoritmo, servono controlli sulla qualità dei dati e sulle elaborazioni logiche e, inoltre, adeguate cautele per ridurre i rischi per gli interessati e per evitare erronee rappresentazioni della capacità contributiva. L'associazione del fattore umano alla tecnologia potrebbe essere la via giusta da seguire per migliorarne le potenzialità e favorire una percezione positiva dei cittadini.

Sempre a tal proposito viene in evidenza un'altra problematica correlata alle precedenti, cioè quella della pseudonimizzazione. La legge di bilancio, nello specifico, prevede che verrà messo in atto quanto previsto dall'articolo 24 del GDPR. Prima di poter utilizzare i dati dell'anagrafe dei rapporti finanziari, ossia il flusso di denaro che viene movimentato a nome del contribuente tra vari conti correnti e investimenti, la Guardia di Finanza dovrà mettere in atto processi di pseudonimizzazione, in modo da renderli non identificabili. I profili dei contribuenti e i loro dati finanziari, verranno collegati ad un numero seriale univoco, che potrebbe servire in un secondo momento. Solo nel caso in cui dovessero emergere dei profili di rischio, la Guardia di Finanza e l'Agenzia delle Entrate potranno procedere al percorso inverso, ricollegando il seriale al profilo personale del contribuente e dando così avvio ad indagini più approfondite. Il tutto, come già ampiamente ripetuto, senza che i contribuenti possano sapere come i sistemi informatizzati messi a punto dalle Autorità utilizzino i loro dati.

In riferimento alla tecnica utilizzata sono piovute ampie critiche da parte del Garante, che, a tal proposito, ha espresso parere negativo in quanto la mera sostituzione del nome e del cognome dei contribuenti con una cifra identificativa non tutelerebbe la privacy dei contribuenti. Infatti, questa tecnica non risulterebbe una garanzia di tutela funzionale agli obiettivi dell'Agenzia. Essa prevede la conservazione dei dati personali in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive e per cui non sarebbe una garanzia della riservatezza dei dati. Sarebbe soltanto, quindi, una misura di sicurezza non risolutiva, innanzitutto perché, in ragione del dettaglio delle informazioni che sarebbero associate allo pseudonimo in luogo del codice fiscale, l'interessato risulterebbe comunque identificabile. Infatti, i dati anche se pseudonimizzati non perdono la loro caratteristica di dati personali, riferendosi comunque a persone fisiche identificabili, anche se solo indirettamente.

Inoltre l'individuazione delle posizioni da sottoporre a controllo ha proprio l'obiettivo di identificare il contribuente, quindi la misura prevista contrasterebbe con la finalità perseguita e risulterebbe solo un inutile aggravio per l'Agenzia delle Entrate.

4. Limiti ai diritti dell'interessato

La nuova legge di bilancio, andando a modificare l'art. 2 undecies del D.Lgs. n. 196/2003 del Codice in materia di protezione dei dati personali, va a limitare ulteriormente l'esercizio dei diritti dell'interessato, tutelati dagli artt. 15-22 del GDPR, applicando le limitazioni anche alle attività di prevenzione e contrasto all'evasione fiscale. I contribuenti interessati non potranno cioè esercitare, fra gli altri, né il diritto di accesso alle proprie informazioni personali oggetto di trattamento, né richiedere la loro correzione o cancellazione nel caso in cui le stesse risultino errate o incomplete. Si tratta di una misura forte che assimila la lotta all'evasione alle altre priorità relative all'interesse e all'ordine pubblico per le quali è possibile limitare il diritto dei cittadini alla tutela e riservatezza dei loro dati personali.

Il Garante ha sottolineato che la preclusione dell'esercizio dei diritti, innanzitutto, risulta in contrasto con lo Statuto dei diritti del contribuente, che regola i rapporti tra l'amministrazione finanziaria ed i contribuenti in base ai principi di massima trasparenza. Tra l'altro c'è anche da considerare il fatto che queste ulteriori limitazioni potrebbero essere un'arma a doppio taglio per il Fisco, in quanto non darebbero più la possibilità al contribuente di rettificare, correggere o richiedere la cancellazione dei propri dati, che quindi resterebbero inesatti o illegittimamente acquisiti esponendo l'amministrazione ad ingenti richieste risarcitorie oltre che a sanzioni amministrative. Inoltre è lo stesso GDPR a specificare che anche le limitazioni devono rispettare l'essenza dei diritti e delle libertà fondamentali oltre che configurarsi come misura necessaria e proporzionata.

Difatti l'Autorità Garante aveva avanzato la proposta di circoscrivere la portata delle limitazioni disposte dalla norma in oggetto per renderla conforme all'art. 23 del GDPR (escludendo, ad esempio, dalle limitazioni l'esercizio del diritto di rettifica o l'integrazione dei dati di carattere valutativo, la richiesta di cancellazione dei dati inesatti o illecitamente raccolti e/o conservati). La soluzione auspicata nella memoria del Garante su questo tema era una limitazione dei diritti analoga a come già previsto, ad esempio, in ambito antiriciclaggio[83]. Infatti, all'art. 39 del D.Lgs. n. 231/2017 le misure vengono, circoscritte con l'individuazione di fasi del procedimento in cui i diritti

[83] A. FONTANAROSA, Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali, in "*La Repubblica*", 4 ottobre 2019.

dei cittadini sono limitati, senza un impedimento generalizzato, come accade con la nuova norma sui controlli fiscali.

Sulla base di queste considerazioni, non ci sono dubbi sul fatto che i diritti possano essere limitati solo in caso di un pregiudizio effettivo e concreto alle esigenze pubbliche perseguite, da definire in maniera chiara e, soprattutto, nei limiti di quanto necessario e proporzionato in una società democratica. Le nuove misure inserite nella legge di bilancio pongono, quindi, sui piatti di una stessa bilancia da un lato il rilevante interesse pubblico e dall'altro i diritti dei contribuenti in ambito privacy, andando ad effettuare una operazione di bilanciamento, che come spesso accade, non risulta assolutamente semplice.

5. Conclusioni

Alla luce della nuova legge di bilancio, l'utilizzo di strumenti tecnologici a disposizione dell'Agenzia delle Entrate e della Guardia di Finanza rappresenta sicuramente un aspetto rilevante nella lotta alla prevenzione e al contrasto delle frodi e dell'evasione fiscale. Ciò nonostante, come già ampiamente affrontato, la disciplina necessita di essere allineata alla normativa europea in materia di protezione e trattamento dei dati personali di cui al GDPR.

È forse oggi il caso di riflettere approfonditamente per capire realmente fin dove ci si vuole spingere e quanto si vuole sacrificare della propria privacy a fronte di quello che oggi è diventato a tutti gli effetti un rilevante interesse pubblico finalizzato alla prevenzione e al contrasto dell'evasione fiscale. Come più volte affermato dal Garante italiano per il trattamento dei dati personali, la privacy non vuol costituire un ostacolo nella strada verso il contrasto all'evasione fiscale, infatti "*il Garante ha sempre supportato le misure volte a rafforzare l'efficacia dell'azione di contrasto dell'evasione fiscale, nella ricerca del miglior equilibrio tra la funzionalità delle verifiche e il diritto alla protezione dei dati personali. Le misure prescritte dall'Autorità hanno contribuito a migliorare l'incisività dell'azione di contrasto dell'evasione, minimizzando il rischio di attacchi informatici al prezioso patrimonio informativo dell'Agenzia delle Entrate e garantendo la buona riuscita degli accertamenti attraverso l'esattezza dei dati (e quindi l'affidabilità della profilazione) sui quali essi si basano*".

LA MANCATA NOMINA DEL RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI PER I SOGGETTI PRIVATI

di Gaetano Guarino

SOMMARIO: 1. Introduzione; - 2. L'obbligo di nomina del responsabile per la protezione dei dati; - 3. Casi di esenzione dalla nomina; - 4. I doveri del RPD; - 5. Casistica giurisprudenziale; - 6. Rilievi critici.

Quest'articolo illustra le vicende relative alla nomina del responsabile per la protezione dei dati personali. Dopo aver passato in rassegna le norme che ne prevedono l'istituzione ed i possibili casi di esenzione, si passa a delinearne i compiti. Si prosegue analizzando alcuni casi giurisprudenziali relativi all'ipotesi della sua mancata nomina. Nelle osservazioni finali si sollevano dei rilievi critici.

1. Introduzione

L'oggetto del presente lavoro riguarda la figura professionale del responsabile per la protezione dei dati personali c.d. data protection officer o RPD[84], disciplinata dal regolamento europeo per la protezione dei dati personali 679/2016[85] UE agli art. 37, 38 e 39.

Si tratta di una figura professionale dedita a concretizzare le norme previste dal Reg. in atti e/o fatti, al fine di garantire la protezione dei dati personali dei soggetti che vengono trattati dall'ente pubblico e/o privato da cui lo stesso è stato nominato. I suoi compiti riguardano la vigilanza sul rispetto di quel complesso di diritti e doveri stabiliti dal Reg., da cui derivano l'applicazione di specifiche misure a carico del titolare e del responsabile del trattamento. Il suo impiego si inserisce nell'ambito di quelle condotte di carattere preventivo finalizzate a rendere effettiva la tutela della riservatezza e ad evitare sanzioni a carico dei soggetti tenuti al rispetto della normativa di settore. Il suo

[84] Di seguito denominato solo RPD.
[85] Di seguito denominato Reg.

contributo pertanto è di carattere prettamente tecnico professionale, come se fosse un perito della riservatezza[86].

2. L'obbligo di nomina del responsabile per la protezione dei dati.

Il Reg. all'art. 37 stabilisce i casi tassativi in cui deve essere effettuata la nomina del RPD.
Innanzitutto nelle pubbliche amministrazioni, ad eccezione degli uffici giudiziari nell'esercizio delle loro funzioni giurisdizionali.
Secondariamente quando le attività principali del titolare e del responsabile del trattamento dei dati personali per loro natura, ambito di applicazione e/o finalità richiedono il monitoraggio regolare e sistematico di dati personali su larga scala, ovvero hanno ad oggetto dati sensibili su larga scala, o relativi a condanne penali o reati.
Inoltre il Reg. lascia aperta la possibilità che la legislazione di uno stato membro, o quella del diritto dell'Unione Europea preveda ulteriori ipotesi della sua nomina come obbligatoria.
Il dovere di nomina del RPD è presidiato da un'elevata sanzione. Infatti l'art. 83 com.4 lett. a) del Reg. prevede una sanzione amministrativa pecuniaria fino a €10 000 000, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nell'ipotesi in cui vi sia la violazione dell'art. 37 del Reg., che appunto prevede la nomina obbligatoria del RPD.

3. Casi di esenzione dalla nomina.

Interpretando l'art. 37 del Reg. a contrario risulterebbe facoltativa la nomina del RPD nei casi in cui via sia un soggetto privato che nello svolgimento della sua attività principale non effettua trattamenti su larga scala, ovvero riguardanti dati sensibili, condanne penali o reati. Si tratterebbe pertanto di piccoli enti che trattano modesti volumi di dati personali.

[86] Ex. Art 37 com. 5 Reg.: "*Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*".

Tuttavia non vi è una norma espressa al riguardo, così come vi è invece per la tenuta dei registri delle attività di trattamento. Infatti il Reg. all'art.30 par. 5 prevede l'esenzione della tenuta di questi registri nelle aziende con meno di 250 dipendenti, salvo che il trattamento non presenti un rischio per i diritti e le libertà dell'interessato, non sia occasionale, o riguardi dati sensibili.

Quindi discrimen che sembrerebbe utile ad orientare l'interprete è quello della presenza, o meno, di dati sensibili come oggetto del trattamento.

Essi sono elencati nell'art. 9 del Reg.: l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici o biometrici intesi a identificare in modo univoco una persona fisica, quelli relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. A cui si aggiungono i dati relativi a condanne penali o reati. Si precisa che sebbene lo stesso art. 9 vieti il trattamento di tali dati in via di principio, esso prevede diverse eccezioni ad es.: motivi sanitari e l'ipotesi in cui l'interessato abbia reso pubblici tali dati.

Data la delicatezza della questione è intervenuto il comitato europeo sulla protezione dei dati personali (EDPB) emanando linee guida uniformi[87] anche sull'interpretazione delle seguenti terminologie: attività principale, trattamento su larga scala e monitoraggio regolare e sistematico.

Riguardo l'attività principale[88] il comitato partendo dal considerando 97 del Reg. che recita "Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria" giunge a stabilire che con tali attività si intendono quelle operazioni essenziali necessarie al raggiungimento degli obiettivi del titolare, o del responsabile.

Ad esempio nell'attività sanitaria l'attività principale è l'assistenza sanitaria, che non sarebbe possibile senza il trattamento dei dati personali contenuti nelle cartelle cliniche. Pertanto tali informazioni sono parte essenziale delle attività principali e quindi gli ospedali sono tutti tenuti alla nomina del RPD[89].

[87] Si tratta delle *Linee guida sui responsabili della protezione dei dati*, emanate dal gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 13 dicembre 2016 ed emendate il 30 ottobre 2017, disponibili sul sito della Commissione Europea all'indirizzo: *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048*

[88] Ex linee guida cit. punto 2.1.2. pag.9.

[89] Secondo il comitato questo vale anche per un'azienda che svolge attività di sorveglianza.

Invece si evidenzia che le attività relative al pagamento dei dipendenti o alla predisposizione di supporti informatici rientrano tra le attività accessorie, non utilizzabili come indicatore dell'obbligo di nomina del RPD.

Riguardo il trattamento su larga scala[90] il comitato prende spunto dal considerando 91 del Reg. che definisce tali trattamenti come quelli: "che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

Poi prende atto dell'impossibilità di stabilire la quantità di dati, o il numero di interessati coinvolti, ma raccomanda di tener conto di alcuni indicatori: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuali della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati; la durata, ovvero la persistenza, del trattamento.

Oltre a ciò elenca alcune ipotesi di trattamenti su larga scala: quelli dei pazienti negli ospedali, quelli riguardanti gli spostamenti dei soggetti che usufruiscono del trasporto pubblico; quelli dei dati di geolocalizzazione raccolti in tempo reale per finalità statistiche per una catena internazionale di fast food; quelli effettuati da banche, o assicurazioni[91].

Al contrario non sono considerati su larga scala quei trattamenti relativi a pazienti svolti da un singolo professionista sanitario, o quelli relativi a condanne penali e reati svolto da un singolo avvocato.

Per quel che concerne la definizione di monitoraggio regolare e sistematico[92] il comitato comincia la sua analisi dal considerando 24 del Reg. che parla di "monitoraggio del comportamento di detti interessati" includendovi il tracciamento e la profilazione per finalità di pubblicità comportamentale. Procede osservando che la nozione di monitoraggio non riguarda solo l'online e che il tracciamento va considerato solo uno dei possibili esempi di monitoraggio del comportamento.

Il monitoraggio è "regolare" quando avviene in modo continuo, ovvero a intervalli definiti per un arco di tempo definito; o ancora quando è ricorrente o ripetuto a intervalli costati e avviene cioè in modo costante o a intervalli periodici.

[90] Ex linee guida cit. punto 2.1.3. pag.9.
[91] Il comitato cita come esempi anche i trattamenti effettuati da motori di ricerca per finalità di pubblicità comportamentale; infine il trattamento di dati (metadati, contenuti ed ubicazione) da parte di fornitori di servizi telefonici, o telematici.
[92] Ex linee guida cit. punto 2.1.4. pag.11.

Mentre per sistematico i significati da considerare sono: che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati, svolto nell'ambito di una strategia.
Gli esempi offerti dal comitato sono: la manutenzione di una rete di telecomunicazione, o la prestazione di servizi di telecomunicazioni; il reindirizzamento di e-mail; l' attività di marketing basate sull'analisi di dati; la profilazione e lo scoring per valutare il rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili[93].

4. I doveri del RPD.

Per delineare gli obblighi del RPD è necessario premettere, per linee generali, i compiti che gravano su responsabile e titolare del trattamento.
Principalmente il titolare ha l'obbligo di comunicare, a coloro che conferiscono i loro dati personali per un trattamento (c.d. soggetti interessati), una serie di precise e puntali informazioni[94], le quali devono essere espressamente fornite in modo chiaro e trasparente[95] alla prima comunicazione utile e sono, a titolo esemplificativo e non esaustivo: identità ed i contatti di responsabile e/o titolare del trattamento, la finalità per cui vengono utilizzati i dati, la base giuridica, i destinatari dei dati personali, la volontà o meno di trasferire i dati al di fuori dello SEE, la durata della loro conservazione[96] e se sarà svolto, o meno, un processo automatizzato.
In particolare dovrà essere predisposto il dove ed il quando il titolare e/o responsabile richiedono il rilascio del consenso[97] per il trattamento dei dati e l'accettazione dell'interessato.

[93] Altri esempi citati dal comitato sono: i programmi di fidelizzazione, la pubblicità comportamentale, il monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; l'utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.
[94] Ex. Art. 13 del Reg. se sono state raccolte presso l'interessato, ex. Art. 14 se le informazioni non sono state ottenute presso l'interessato. Si è preferito elencare quelle ex. art. 14 perché differiscono solo leggermente da quelle contenute nella disposizione precedente, contengono solo qualche informazione in aggiunta rispetto al quelle del precedente articolo data la necessità di garantire maggiormente l'interessato.
[95] Ex art.12 Reg.
[96] o i criteri per determinarla.
[97] Ex Art.7 Reg.

Inoltre devono essere comunicati i diritti dei soggetti interessati[98]: l'accesso, la rettifica, la cancellazione, la limitazione, l'opposizione, la portabilità ed il reclamo nonché la possibilità di revocare il consenso.

Secondariamente in ogni ente in cui si verifica il trattamento di dati personali deve essere tenuto un registro dei trattamenti in base a quanto disposto dall'art. 30 del Reg.

In aggiunta il titolare deve porre in essere misure di sicurezza adeguate finalizzate a tutelare, gestire e custodire i dati personali, garantendo un livello di sicurezza adeguato al rischio[99]. Nello specifico il Reg.[100] prevede alcuni esempi di misure di sicurezza adeguate, come la pseudominizzazione[101] e la cifratura dei dati, nonché misure atte a garantire la riservatezza, l'integrità, la disponibilità e la resilienza di sistemi e servizi. Oltre a questo deve essere garantita la possibilità di ripristino in caso di incidente, nonché una procedura per verificare l'efficacia delle misure, considerando i rischi per la perdita, la distruzione, la modifica, e la divulgazione delle informazioni.

In altre parole il titolare ha il dovere di porre in essere tutte le misure tecniche per salvaguardare i diritti e le libertà delle persone interessate.

Il responsabile del trattamento[102] oltre a essere colui che effettua il trattamento per conto del titolare è tenuto ad un'attività latu senso collaborativa con il titolare per la tutela dei dati. Infatti egli deve garantire che le misure tecniche ed organizzative da lui predisposte soddisfino i requisiti regolamentari e tutelino i diritti dell'interessato, ma anche prestare assistente tecnica ed organizzativa al titolare. Inoltre è tenuto a cancellare, o restituire, i dati dopo il trattamento su richiesta del titolare e a fornire le informazioni necessarie per dimostrare il rispetto degli obblighi regolamentari, nonché alla collaborazione nei casi di attività di ispezione e/o verifica.

Quindi l'attività di vigilanza del RPD verte principalmente su queste attività: quella informativa, quella relativa alla custodia dei registri e quella riguardante gli obblighi di sicurezza, ma più in generale sul rispetto di quanto previsto complessivamente dalla normativa di settore.

Alla luce del complesso di diritti e doveri presenti in un ente in tema di protezione dei dati, il RPD è espressamente tenuto a sensibilizzare tutti soggetti che vi lavorano, in

[98] Ex art. 15, 16, 17, 18, 19 e 20 Reg.
[99] Ex art. 24 Reg.
[100] Ex. Art. 25 Reg.
[101] Ex art. 32 Reg.
[102] Ex art. 28 Reg.

particolare coloro che effettuano i trattamenti dei dati e sono tenuti alla loro custodia[103]. Particolare attenzione egli dovrà rivolgere ai diritti degli interessati, perché tutte le norme in materia sono espressione del loro diritto fondamentale alla riservatezza[104]. Oltre a ciò egli è il punto di contatto tra l'ente e l'autorità di vigilanza per la protezione dei dati personali, alla quale la sua nomina deve essere comunicata[105]. Infine egli è tenuto a fornire un parere in merito alla valutazione di impatto.

In sostanza il RPD ha il compito di far porre in essere tutte le misure previste dal Reg. che altrimenti rischierebbero di rimanere lettera morta. Tant'è vero che egli deve essere adeguatamente coinvolto in tutte le questioni in tema di protezione dei dati personali[106].

Nei suoi confronti il titolare ed il responsabile del trattamento devono garantire il suo regolare operato[107]. Pertanto il Reg. prevede che gli stessi sono tenuti a fornire al RPD le risorse necessarie per assolvere tali compiti e a garantire l'accesso ai dati e ai trattamenti per mantenere la sua conoscenza specialistica. Inoltre non devono ostacolarlo, né fornirgli istruzioni riguardo l'esecuzione dei suoi compiti, né sanzionarlo in alcun modo per l'adempimento dei suoi doveri.

D'altro canto l'RPD è tenuto a riferire solo ai vertici del titolare dell'ente, o del responsabile del trattamento e a serbare il segreto e/o la riservatezza sul suo operato[108]. La sua posizione di terzietà è salvaguardata anche dal fatto che nel caso in cui egli svolga anche altri compiti nell'ente, il titolare e il responsabile devono garantire che non vi siano conflitti di interesse[109].

5. Casistica giurisprudenziale

Vi sono stati pochi casi in cui l'autorità di vigilanza sulla protezione dei dati ha sanzionato enti che non hanno nominato il RPD.

---

[103] Ex. Art. 39 par. 1 Lett. (a.
[104] Ex Art. 8 Carta dei diritti fondamentali dell'Unione Europea ed ex art. 8 della Convenzione Europea per la salvaguardia dei diritti dell'uomo.
[105] Art. 37 par. 8 Reg.
[106] Ex. Art. 38 com. 1: *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".*
[107] Ex. Art. 38
[108] Ex. Art. 38 com. 5.
[109] Ex. Art. 38 com. 6.

Innanzitutto in Germania l'autorità di vigilanza (BfDI) ha sanzionato un fornitore di servizi di comunicazione per mancata nomina del RPD, nonostante le preventive richieste della stessa autorità di ottemperare alla nomina. La sanzione è stata di € 10.000, solo perché l'ente rientra nella categoria delle microimprese[110].

Un altro caso si è verificato in Austria[111], dove l'autorità ha sanzionato una società del settore sanitario con una sanzione di €50.000 per non aver soddisfatto né le norme riguardanti le informazioni sulla riservatezza da fornire né la nomina del RPD.

Un'ipotesi particolare è avvenuta in Spagna[112], dove l'autorità ha sanzionato per €25.000 la società sviluppatrice della celebre app GLOVO: la Glovoapp 23 SL.

La società sosteneva che la sua attività non rientrava tra i casi di nomina obbligatoria del RPD, perciò non aveva effettuato la nomina e conseguentemente non aveva indicato i relativi dati di contatto sul sito. Invece nel corso dell'istruttoria il garante ha accertato che la nomina fosse obbligatoria, perché si trattava di un'attività che prevedeva il monitoraggio regolare e sistematico dei soggetti interessati su larga scala. Infatti quest'attività si svolge su un'ampia area geografica (il servizio è diffuso in più di 200 città), il numero degli interessati è molto alto, viene effettuata la profilazione, con diverse tipologie di dati, tra cui quelli di geolocalizzazione ed addirittura quelli riguardanti le abitudini di consumo alimentare. Si evidenzia che si tratta di un'ipotesi di monitoraggio, (oltre che su vasta scala) regolare e sistematico, così come indicato nelle linee guida sopracitate, che citano tra gli esempi proprio il tracciamento dell'ubicazione da parte di app su dispositivi mobili.

In Italia il garante ha agito in modo simile in due casi.

Il primo[113] riguardava l'azienda sanitaria provinciale di Cosenza. Nel corso di un'istruttoria relativa alla mancata omissione di dati personali su documenti pubblicati sul sito web dell'ente è emersa la mancata comunicazione della nomina del RPD. Si è scoperto che era stato nominato un soggetto che poi era andato in pensione e non si

---

[110] FONTE: LABOR PROJECT S.R.L., *GDPR, solo 2 sanzioni nell'Ue per la mancata nomina del DPO*, *https://www.key4biz.it/gdpr-solo-2-sanzioni-nellue-per-la-mancata-nonima-del-dpo/285229/*,13 gennaio 2020.

[111] FONTE: LABOR PROJECT S.R.L., *GDPR, solo 2 sanzioni nell'Ue per la mancata nomina del DPO, https://www.key4biz.it/gdpr-solo-2-sanzioni-nellue-per-la-mancata-nonima-del-dpo/285229/*,13 gennaio 2020.

[112] FONTE: MORRI ROSSETTI, L'*Autorità spagnola per la protezione dei dati personali sanziona Glovo per mancata nomina del DPO,* in Osservatorio Data Protection, *https://www.osservatorio-dataprotection.it/2020/06/23/lautorita-spagnola-per-la-protezione-dei-dati-personali-sanziona-glovo-per-mancata-nomina-del-dpo/,* 23 giugno 2020.

[113] Garante della Privacy, provvedimento n. 173 del 1ottobre 2020, doc. web. N. 9483375, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9483375*

era provveduto ad una nuova nomina. L'autorità ha evidenziato che, seppur temporaneamente, doveva essere individuato un sostituto. Sebbene nel corso dell'istruttoria l'ASL abbia pubblicato un numero di telefono ed un indirizzo PEC dell'ufficio gestione privacy, la stessa è stata condannata ad una sanzione di €30.000.

Il secondo caso[114] riguardava il comune molisano di Pettoranello in provincia di Isernia. Un ex dipendente comunale lamentava una presunta violazione della riservatezza dovuta all'invio del comune presso la sua casella pec di provvedimenti a lui riguardanti. Lo stesso aveva chiesto più volte di inviare comunicazioni presso altro indirizzo pec o brevi manu. Nel corso dell'istruttoria è emersa l'assenza di nomina del RPD del comune. L'ente si è giustificato lamentando l'assenza di personale e che la nomina era stata effettuata con l'affissione nella bacheca comunale e la pubblicazione del relativo decreto sul suo sistema telematico, senza la comunicazione al garante. Pertanto lo stesso si considerava in buona fede.

Il garante ha ritenuto che la pubblicazione della nomina sul sito web mira a garantire che gli interessati possano contattare l'RPD in modo facile e diretto. Pertanto le altre modalità non sono state considerate idonee a soddisfare tale obbligo. In particolare la pubblicazione della relativa delibera non prova la nomina, perché non consente di capire se sono stati pubblicati i dati contatto del RPD nella stessa e se il generico richiamo al sistema telematico fa riferimento al sito dell' ente. Tuttavia la pubblicazione tardiva del nominativo sul sito dell'ente ha convinto il garante a sanzionare lo stesso con la mera ammonizione e non con la sanzione pecuniaria in quanto violazione minore ai sensi dell'art. 83 par.2 del Reg.

6. Rilievi critici.

Da uno sguardo complessivo sulla questione emerge che il responsabile della protezione dei dati possa essere il vero punto di riferimento per un ente in materia di protezione dei dati personali, colui che fornisce tutte le informazioni utili al fine di rispettare le norme in materia ed evitare sanzioni. Per agevolarlo è stata emanato un vero e proprio manuale d'istruzione[115]. Data la complessità della normativa ed i molteplici diritti

[114] Garante della Privacy, provvedimento n.56 del 12 marzo 2020, doc. web. N. 9429218, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9429218*

[115] Douwe KORFF e Marie GEORGES, Manuale RPD Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea, con il contributo del Garante italiano per la protezione dei dati personali

e doveri derivanti, creare la figura di un esperto equivale a creare una guida per i molti soggetti tenuti al rispetto delle norme, ma che possono essere sprovvisti delle competenze tecniche e professionali per garantirne l'applicazione.

Riguardo le sanzioni per la sua mancata nomina, queste sembrano per lo meno opinabili quanto alla loro eccessiva gravità, se si considera che la mancata nomina, così come la mancata comunicazione della nomina può avvenire per una molteplicità di ragioni. Quindi le autorità dovrebbero ben svolgere il contraddittorio e considerare tutti i fattori intervenuti in ogni singola vicenda per ben calibrare le sanzioni.

Tuttavia nessun ente può considerarsi assolto dai suoi obblighi con la semplice indicazione di un nominativo su un sito web. Questo perché lo scopo principale sotteso a tutta la normativa è di garantire una tutela effettiva e concreta dei diritti degli interessati, la quale non si esaurisce con una semplice nomina, o la sola fornitura delle relative informazioni, ma riguarda anche la gestione e conservazione dei dati personali in ogni fase del trattamento.

Pertanto appare necessaria una continua e puntuale opera di sensibilizzazione e formazione di tutte le tipologie di enti e di soggetti che possono essere coinvolti nel trattamento dei dati personali. Infatti innalzare la riservatezza a diritto fondamentale significa avere dato alla stessa lo status di un diritto, rafforzato e fortemente privilegiato rispetto agli altri e questo proprio in ragione della sua importanza, che se non altro deriva dal fatto che ci riferiamo ad un diritto che coinvolge ogni giorno ed ogni momento milioni di individui, che utilizzano le attuali tecnologie e non solo.

Tuttavia non bisogna lasciarsi trascinare dalla tentazione di introdurre norme su norme ed obblighi su obblighi, altrimenti si rischia l'effetto opposto: il mancato rispetto delle stesse giustificato dall'incapacità ed impossibilità di controllarne il rispetto da parte delle autorità competenti.

L'RPD pertanto è tenuto a far comprendere l'importanza della materia e a realizzare quei piccoli e grandi interventi che garantiscono la tutela della riservatezza. Al contempo le autorità di vigilanza, gli enti professionali e di categoria dovrebbero continuare, in modo costante, la loro opera di formazione e sensibilizzazione in materia di protezione dei dati personali.

---

e altri Partner del progetto, accessibile sul sito del garante per la protezione dei dati personali: *https://www.garanteprivacy.it/documents/10160/0/T4DATA+-+Manuale+per+gli+RPD.pdf/bdea3d2d-7bfc-80c5-8f1c-f8c567b44e50?version=1.1*

DIRITTO ALLO STUDIO, NUOVE TECNOLOGIE PER LA DIDATTICA E PRIVACY

Francesco Lo Chiatto

SOMMARIO: 1. Diritto allo studio come principio fondamentale - 2. La privacy nella scuola - 3. La tecnologia e le nuove metodiche di apprendimento - 4. Didattica a distanza e privacy ai tempi del Covid - 5. Conclusioni

This work concerns the right to study related to the use of new technologies for distance learning, with specific reference to the protection of the privacy of users of the service. The right to study finds its reference in numerous International and European Papers, but above all in articles 3-33-34 of the Italian Constitution. In school, privacy plays a decisive role, for the protection of the fundamental values of the individual person. Privacy takes on an even more important aspect when there is a use of new technologies for distance learning, which could be more invasive than the personal sphere of the individual pupil. The intervention of the Privacy Guarantor was fundamental for a greater clarification on the correct use of online platforms for distance learning during Covid-19.

1. Diritto allo studio come principio fondamentale

Il diritto allo studio rientra tra i diritti fondamentali e inalienabili della persona, così come sancito nella Dichiarazione universale dei diritti dell'uomo (Onu, 10 dicembre 1948). L'art. 26 di questa Dichiarazione afferma che ogni individuo ha diritto all'istruzione, che deve essere gratuita e obbligatoria almeno per le classi elementari. L'istruzione tecnica e professionale, invece, deve essere accessibile a tutti, così come l'istruzione superiore. Il diritto allo studio ha lo scopo di garantire il pieno sviluppo della personalità umana insieme al rispetto dei diritti e delle libertà fondamentali di ognuno, tali da promuovere la comprensione, la tolleranza, l'amicizia tra Nazioni, gruppi razziali e religiosi, così come affermato dall'art. 2 della Convenzione europea dei diritti

dell'uomo protocollo 1[116] che riconosce come fondamentale il diritto allo studio che non può essere negato a nessuno. Lo Stato deve rispettare il diritto dei genitori di provvedere all'educazione e all'insegnamento dei figli, secondo le proprie convinzioni religiose e filosofiche. L'Italia nella sua Costituzione, all'art.33[117] detta norme generali sull'istruzione ed istituisce scuole, per tutti gli ordini e gradi di apprendimento. Gli enti privati hanno il diritto di istituire scuole ed istituti di educazione, senza oneri per lo Stato, prevedendo tra l'altro un trattamento equipollente a quello degli alunni delle scuole statali. Lo stesso art. 34 della Costituzione Italiana[118], specifica che la scuola è aperta a tutti e che l'istruzione inferiore è impartita almeno per otto anni, ed è obbligatoria e gratuita. Il diritto allo studio viene garantito a tutti, anche a coloro privi di mezzi, in quanto a tutti deve essere data l'opportunità di raggiungere i gradi più alti degli studi, attraverso borse di studio, assegni alle famiglie, a prescindere dalle condizioni socio-economiche di partenza.[119]

2. La privacy nella scuola

Le scuole sono il luogo in cui sin da piccoli si acquisiscono fondamentali strumenti culturali e sociali, si sviluppano le capacità cognitive e sono il luogo basilare per una corretta formazione. In tale contesto, la privacy assurge a baluardo per una corretta tutela dei valori fondamentali della persona e in particolare per i minori. Le scuole, ai

[116] Corte Europea dei diritti dell'uomo, *Guida all'articolo 2 del Protocollo n.1 alla Convenzione europea dei diritti dell'uomo*, aggiornata al 31 dicembre 2018, https://www.echr.coe.int/Documents/Guide_Article_2_Protocol_1_ITA.PDF

[117] Art. 33 Cost: *"L'arte e la scienza sono libere e libero ne è l'insegnamento.*
La Repubblica detta le norme generali sull'istruzione ed istituisce scuole statali per tutti gli ordini e gradi.
Enti e privati hanno il diritto di istituire scuole ed istituti di educazione, senza oneri per lo Stato.
La legge, nel fissare i diritti e gli obblighi delle scuole non statali che chiedono la parità, deve assicurare ad esse piena libertà e ai loro alunni un trattamento scolastico equipollente a quello degli alunni di scuole statali.
E` prescritto un esame di Stato per l'ammissione ai vari ordini e gradi di scuole o per la conclusione di essi e per l'abilitazione all'esercizio professionale.
Le istituzioni di alta cultura, università ed accademie, hanno il diritto di darsi ordinamenti autonomi nei limiti stabiliti dalle leggi dello Stato".

[118] Art. 34 Cost: *"La scuola è aperta a tutti.*
L'istruzione inferiore, impartita per almeno otto anni, è obbligatoria e gratuita.
I capaci e meritevoli, anche se privi di mezzi, hanno diritto di raggiungere i gradi più alti degli studi.
La Repubblica rende effettivo questo diritto con borse di studio, assegni alle famiglie ed altre provvidenze, che devono essere attribuite per concorso".

[119] CATELANI - FALANGA, *La scuola pubblica in Italia*, Brescia, 2011.

sensi dell'art.4.7 GDPR 679/2016[120], sono infatti, titolari del trattamento di tutti i dati che confluiscono in essa, da quelli dei professori, del personale A.T.A., fino a quelli degli alunni, in quanto ne determinano le finalità e i mezzi. Il titolare del trattamento dovrà attuare delle scelte secondo il principio dell'accountability o principio di responsabilizzazione, al fine di tutelare l'interessato. In tale ottica il legislatore con il D.lgs. 101/2018[121] ha abrogato l'Allegato B del Codice Privacy, rubricato "Disciplinare tecnico in materia di misure minime di sicurezza", e quindi non potendosi più parlare di misure minime, occorre assicurare la massima tutela dei dati. Ogni istituto scolastico, pertanto, dovrà porre in essere un Registro del Trattamento, aggiornare informative privacy[122], nominare eventuali Responsabili del Trattamento[123], farsi coadiuvare nelle attività privacy dalla consulenza di un DPO, porre in essere una Dpia, al fine di una corretta valutazione e gestione dei rischi connessi al trattamento e, infine, dare corrette istruzioni e formazione ai suoi dipendenti sulle modalità del trattamento e tenuta dei dati. Un elemento fondamentale nell'assetto privacy, così come citato prima, risulta essere il registro dei trattamenti, così come precisa il Miur, con nota n.877 del 03.08.2018, con la quale ha trasmesso uno schema di tale Registro dei trattamenti per le istituzioni scolastiche, fornendo una guida operativa e una nota metodologica, per la compilazione dello stesso. Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali, oppure quelli espressamente previsti dalla normativa di settore e per tali trattamenti non sono tenute a chiedere il consenso degli studenti o dei genitori.

La scuola deve conservare le informazioni riguardanti gli alunni e deve dare loro la possibilità di rettificarle se erronee o non aggiornate. Nell'era degli smartphone, dei social network, delle foto scattate e condivise istantaneamente, dove un singolo scatto può divenire virale e ledere la dignità di uno o più soggetti, risulta fondamentale analizzare tale fenomeno all'interno degli istituti scolastici e porre in essere misure a tutela

[120] Art. 4.7 GDPR: *"titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"*

[121] D.lgs. 101/2018*: https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg*

[122] Garante della Privacy, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali,* in *https://www.garanteprivacy.it/regolamentoue/informativa*

[123] Garante della Privacy, *Privacy: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche*, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/49205*, 11 dicembre 1997.

della privacy. La scuola con apposito regolamento deve predisporre specifiche disposizioni per un corretto utilizzo degli smartphone, durante l'orario scolastico, al fine di evitare che vi sia una diffusione di registrazioni o immagini, senza che le stesse siano precedute dal consenso di professori e/o studenti. Gli allievi con D.S.A., possono liberamente utilizzare strumenti didattici, che consentano loro anche di registrare durante la lezione, "i c.d. strumenti compensativi e aumentativi", in base alla normativa di settore, L. n. 170/2010[124], senza chiedere il consenso delle persone coinvolte nella registrazione. Per la ripresa di recite, saggi e gite scolastiche, tuttavia, non sarà necessario il consenso delle persone inquadrate, se il solo utilizzo sarà quello familiare o amicale. Diversamente, per una pubblicazione sui social network sarà necessario il consenso degli inquadrati o degli aventi potestà genitoriale, se minori. Altro punto nodale relativamente alla privacy degli alunni è la pubblicazione degli esiti degli scrutini o degli esami in modalità pubblica. A tal proposito, il Miur, ha confermato la pubblicità di tali dati, evitando al contempo, però, di fornire condizioni di salute o altri dati non pertinenti degli studenti, così come non vanno inseriti nei tabelloni, le prove differenziate per gli alunni con disturbi specifici dell'apprendimento. Negli istituti scolastici è facile trovare telecamere installate al fine di tutelare l'edificio con i relativi beni, ma anche in questo caso è di evidente necessità al contempo tutelare le privacy di ogni singola persona inquadrata e in particolar modo degli alunni, che nella maggior parte dei casi sono minori. L'installazione delle telecamere all'esterno degli edifici, deve comunque, sempre garantire il diritto dello studente alla riservatezza e quindi, l'apposizione delle stesse deve risultare strettamente indispensabile al fine di tutelare l'edificio e i beni scolastici, evitando di riprendere i volti degli stessi. Le telecamere, invece, poste all'interno degli istituti, devono essere attivate solo in orario di chiusura con appositi cartelli che riporteranno l'informativa minima e conservate per un tempo non superiore alle 72 ore, salvo non vengano poste a disposizione della polizia o dell'autorità giudiziaria, nel caso di segnalazione di furti, vandalismo o danneggiamenti.
Per una maggiore conoscenza in tema di videosorveglianza l'*European Data Protection Board* ha fornito delle linee guida (3/2019), utili al fine di prevenire trattamento illeciti di dati personali, mentre il Garante Privacy ha predisposto delle FAQ illustrative.

[124] Legge 8 ottobre 2010, n. 170, *Nuove norme in materia di disturbi specifici di apprendimento in ambito scolastico* (10G0192), in *https://www.istruzione.it/esame_di_stato/Primo_Ciclo/normativa/allegati/legge170_10.pdf*

3. La tecnologia e le nuove metodiche di apprendimento

La tecnologia ha modificato e continua a modificare ogni giorno le nostre abitudini, il nostro modo di vivere, il modo di viaggiare e la nostra sicurezza nelle città, in strada e in auto. Le nuove tecnologie oltre ad aver migliorato i servizi alla persona, sono entrate anche nelle vite di queste ultime, cambiando il modo di comunicare e di relazionarsi. Questo processo di cambiamento ha influenzato anche la scuola, infatti, oggi molte informazioni che sono disponibili nella rete internet sono sfruttate anche per studiare e per promuovere un apprendimento significativo. La tecnologia può addirittura rappresentare un terzo insegnante, ovvero una risorsa aggiuntiva in classe, in grado di supportare e aiutare gli alunni nello studio, integrando nel progetto educativo ulteriori informazioni.[125] Possiamo immaginare l'importanza che riveste la tecnologia per bambini con disturbi di apprendimento (DSA), in tal senso infatti, un software può trasformare un lungo testo da leggere in una sintesi vocale da ascoltare, o piuttosto un discorso frontale del docente in una mappa concettuale o in una infografica, ovvero una immagine evocativa da condividere con gli alunni che possono utilizzarla anche a casa per studiare. Le nuove tecnologie in classe permettono di realizzare simulazioni, di viaggiare e orientarsi, di reperire informazioni da fonti diverse e di confrontarle tra loro, di scrivere testi a più mani, in modo cooperativo, di guardare video-tutorial e svolgere esercizi interattivi, e quindi, ci consentono di sperimentare compiti autentici e dinamici, esperienze che prevedono un coinvolgimento attivo da parte degli alunni utilizzando strumenti a loro familiari. La tecnologia impiegata nello studio di alcune discipline è dunque, in grado di integrare l'esperienza dell'apprendimento scolastico e offrire un blocco di partenza per arrivare alla conoscenza significativa. La stessa è in grado di migliorare l'apprendimento quando viene in aiuto a strategie di insegnamento efficaci, compensando difficoltà specifiche.[126] Il problema diffuso di un mancato utilizzo della tecnologia a 360 gradi è che molte scuole mancano di queste strumentazioni, come le LIM, i device, le connessioni a Internet e non tutti i docenti hanno competenze digitali sufficienti per poter sfruttare al meglio questi strumenti digitali. Seppur lentamente, il cambiamento è in atto e nel futuro potremo vedere le scuole colmare

[125] V. PELLEGRINO, S. De CLEMENTE, *Tecnologie dell'istruzione e dell'apprendimento*, Anicia, Roma, 2010.
[126] M. D'ADDAZIO, *Guida al concorso per personale docente della scuola secondaria,* Anicia, Roma, 2020.

il gap con la realtà extrascolastica che potrà usufruire di questa risorsa aggiuntiva, cioè un buon utilizzo della tecnologia ai fini didattici, come supporto per l'apprendimento anche quando si è a casa.[127]

4. Didattica a distanza e privacy ai tempi del COVID

A seguito dell'emergenza Covid-19, con la chiusura delle scuole è nata l'esigenza di garantire comunque la continuità didattica e ciò ha imposto il ricorso a soluzioni innovative come l'utilizzo di strumenti tecnologici, che hanno permesso una didattica a distanza.[128] Ogni alunno attraverso l'utilizzo del proprio pc, collegandosi attraverso piattaforme apposite, condivise con il resto della classe, ha potuto continuare a usufruire della didattica a distanza, D.A.D., anche restando a casa.[129] La prosecuzione dell'attività formativa è stata resa possibile anche grazie al "lodevole sforzo delle istituzioni scolastiche e universitarie, degli studenti e degli stessi genitori", come sottolineato dall'ex Presidente dell'Autorità Garante nella lettera[130], inviata al Ministro dell'Istruzione, al Ministro dell'Università e della ricerca e al Ministro per le pari opportunità e la famiglia. Tuttavia, sottolinea Soro, che è necessario non sottovalutare i rischi che possono derivare da un uso scorretto o poco consapevole degli strumenti telematici, spesso dovuto anche alla loro oggettiva complessità di funzionamento. Non sorprende, infatti, che il Garante abbia ricevuto diversi quesiti e segnalazioni da parte dei DPO degli istituti scolastici, ai quali ha provveduto a dare riscontro con l'approvazione di uno specifico atto di indirizzo[131], nell'intento di fornire un supporto utile alla migliore gestione dei dati personali di tutti i soggetti coinvolti nell'attività didattica a distanza. Con riferimento alla base legale del trattamento dei dati personali effettuato tramite i servizi di didattica online, il Garante chiarisce che scuole e università sono

[127] R. GALATI, *Le tecnologie cambiano l'ambiente di apprendimento,* in *https://it.pearson.com/genitori/primaria/educazione-digitale/tecnologie-cambiano-ambiente-apprendimento.html*
[128] E. BARBUTO, *La didattica a distanza. Metodologie e tecnologie per la Dad e l'e-learning,* Editore Edises, Napoli, 2020.
[129] B. BRUSCHI, PERISSINOTTO, *Didattica a distanza- Com'è, come potrebbe essere,* Editori La Terza, Bari
[130] A. SORO, lettera al Ministro dell'Istruzione, al Ministro dell'Università e della ricerca e al Ministro per le pari opportunità e la famiglia, in *https://www.garanteprivacy.it/documents/10160/0/Lettera+di+Soro+al+Minstro+dell%E2%80%99Istruzione%2C+Universit%C3%A0+e+ricerca.pdf/74a48ed5-245f-4db3-8a3d-8a78749298df?version=1.1*
[131] Garante della Privacy, provvedimento n. 64 del 26 marzo 2020, doc. web n. 9300784, in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9300784*

autorizzate a trattare i dati, anche relativi a categorie particolari , come le informazioni sulle convinzioni religiose o sulla salute, di docenti, alunni, studenti, genitori, poiché il trattamento è riconducibile alle funzioni istituzionalmente assegnate a scuole e atenei e, pertanto, non è necessario richiedere un consenso specifico. Quanto al ruolo dei fornitori, il provvedimento sottolinea che se il trattamento dei dati attraverso la piattaforma viene effettuato per conto della scuola o dell'università, e cioè se l'istituto è nella posizione non soltanto di decidere i mezzi tecnici per trattare i dati personali, ma anche quali dati saranno trattati, a quali dati i terzi avranno accesso, quando tali dati saranno eliminati, e le altre decisioni rilevanti in relazione al trattamento, allora il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico al fine di designarlo responsabile del trattamento. In questo senso l'Autorità evidenzia come sia necessario il rispetto del principio di limitazione delle finalità del trattamento, esortando gli istituti ad accertarsi che i dati trattati per loro conto siano utilizzati esclusivamente per finalità di didattica online, anche fornendo le adeguate istruzioni sul trattamento, che potranno essere incluse all'interno della nomina a responsabile, quali ad esempio quelle sulla conservazione dei dati, nonché sulle procedure di gestione di eventuali violazioni di dati personali. L'Autorità evidenzia come l'attenta selezione e la configurazione adeguata degli strumenti per la didattica online spetti proprio alle scuole e alle università, in quanto titolari del trattamento. Tali scelte – sottolinea il Garante – dovranno conformarsi ai principi di *privacy by design e by default* del GDPR, tenendo conto sia del contesto didattico, che delle finalità di insegnamento legate all'utilizzo dei dati, sia dei rischi connessi per i soggetti coinvolti, che possono essere anche minorenni. In questo senso, il Garante rimarca che è essenziale scegliere con cura la soluzione migliore tenendo conto anche delle garanzie offerte in relazione alla protezione dei dati personali, in quanto, alcune piattaforme offrono servizi ulteriori rispetto a quelli per meri fini didattici. Nel provvedimento l'Autorità si impegna a vigilare sull'operato dei fornitori delle principali piattaforme per la didattica a distanza, ritenendo inammissibile l'operato di alcune di esse, che condizionano la fornitura dei servizi di didattica al rilascio del consenso, da parte dello studente o dei genitori, per l'effettuazione di operazioni ulteriori, preordinate al perseguimento di finalità proprie del fornitore. Alla luce dei rischi specifici connessi all'utilizzo delle piattaforme, potrebbe rendersi necessaria una valutazione d'impatto privacy ai sensi dell'art. 35 del GDPR, per verificare che siano state poste in essere le adeguate misure di sicurezza per limitare i rischi e garantire che il trattamento rispetti i principi del Regolamento

Privacy. Tale analisi, tuttavia, non è richiesta per il trattamento effettuato da una singola scuola nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma, a condizione che non consenta il monitoraggio sistematico degli utenti o comunque non implichi l'utilizzo di soluzioni tecnologiche particolarmente invasive, come la geolocalizzazione o l'uso di dati biometrici. L'Autorità chiarisce inoltre, quanto sia essenziale rendere pienamente consapevoli docenti, studenti e genitori delle caratteristiche del trattamento e delle misure di salvaguardia nonché dei loro diritti in relazione al trattamento. In tal senso è importante notare che il Garante consiglia l'adozione di iniziative di sensibilizzazione per familiarizzare con l'uso degli strumenti e sottolinea al contempo l'esigenza di adottare un approccio trasparente e chiaro, in relazione alle informative privacy. In tal senso un valido supporto può derivare dall'adozione di soluzioni di *legal design*, per assicurare che i contenuti informativi siano veicolati nella maniera più adeguata in base al target, calibrando adeguatamente gli aspetti formali e sostanziali, tenendo conto delle specificità e della consapevolezza dei soggetti di riferimento, siano essi alunni o professori[132].

Il Garante Privacy, a tale proposito, ha scritto una lettera al Ministro dell'Istruzione Azzolina, prendendo in esame il registro elettronico. Tale registro, fornito da soggetti, già responsabili del trattamento, potrebbe rappresentare lo strumento attraverso cui realizzare una parte significativa dell'attività didattica, riducendo così il ricorso ad altre piattaforme, che non sempre si limitano all'erogazione di servizi funzionali all'attività formativa. Il registro elettronico, premette il Garante Soro, è un prezioso strumento di comunicazione tra i docenti e le famiglie, caratterizzato dalla sostituzione dell'attività didattica in "presenza", con quella a "distanza", che necessita di una stretta interazione tra studenti, insegnanti e genitori, alla quale il registro online è sicuramente funzionale. Nei criteri per la scelta degli strumenti tecnologici per le attività da remoto, vanno utilizzati quelli che offrono ampie garanzie per la tutela dei dati personali. Dopo questa breve disamina sul diritto allo studio, sulla privacy nella scuola e sulle nuove tecnologie per una didattica a distanza, è utile riportare a conclusione le parole del Garante Privacy Antonello Soro:

[132] Per una più dettagliata lettura delle indicazioni del Garante privacy sulla didattica a distanza, si veda Garante della Privacy, provvedimento n. 64 del 26 marzo 2020, allegato 1, doc. web n. 9300784, in *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9300784#allegato*

"*Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di internet e in presenza di nuove forme di comunicazione, questo compito diventa ancora più cruciale* – come sottolinea il Presidente dell'Autorità. "*E´ importante* - continua Soro - *riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino*"[133].

Da alcuni mesi si è insediato come Presidente Garante Privacy il Prof. Pasquale Stanzione, che ha sostituito l'uscente Presidente Antonello Soro, che in un'epoca di cambiamento riflettono la lungimiranza di pensiero radicata sempre in quei principi che il legislatore europeo ci ha offerto**.** Secondo il Garante Privacy Stanzione, l'avvento delle nuove tecnologie ha segnato una vera e propria rivoluzione antropologica, ma anche sociale, culturale, politica, economica. Come rispetto a ogni fenomeno "disruptive", il rischio da evitare è quello di un'eterna rincorsa, da parte del diritto, di una tecnica quasi irraggiungibile per velocità e profondità dell'evoluzione. La chiave per il governo dell'innovazione è, invece, proprio quello della duttilità e lungimiranza garantite dal principio di neutralità tecnologica su cui si fonda il GDPR, che con la sua prevalenza dei principi sulle regole consente un adattamento continuo alla materia da regolare. Così per parafrasare il titolo di un noto libro di Stefano Rodotà- la vita è resa compatibile con la regola e il dialogo costante tra le due è il presupposto di un rapporto armonico tra persona, democrazia e digitale. L'apporto antropocentrico alla tecnica, su cui si fonda il GDPR, condiviso dall'Europa su temi importanti come, l'intelligenza artificiale *in primis*, è il fattore essenziale per garantire che il rapporto tra innovazione e privacy si declini in termini sinergici e non conflittuali. È questa una delle sfide principali con cui il Garante si misurerà nei prossimi anni, nella consapevolezza della rilevanza, anzitutto in termini democratici, del diritto la cui cura gli è affidata[134]**.**

[133] Garante della Privacy, *La scuola a prova di privacy,* in *https://www.garanteprivacy.it/scuola*
[134] Intervista a P. STANZIONE, Presidente del Garante per la protezione dei dati personali, *Privacy. La prima intervista al nuovo Garante. Stanzione: Gdpr è garanzia democratica,* in Diritto Mercato Tecnologia, *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9442541*, 30 luglio 2020.

5. **Conclusioni**

A conclusione del presente lavoro è evidente come il diritto allo studio, che risulta essere basilare per ogni essere umano, rifletta appieno le mutazioni del nostro tempo e ciò in relazione alle nuove tecnologie, alla didattica a distanza e al diritto della privacy. Questa diviene pilastro basilare per la tutela dei diritti fondamentali, soprattutto in luoghi, come gli istituti scolastici, in cui vi è un ampio numero di dati particolari, sensibili, da tutelare. La scuola ai sensi dell'art.4.7 del GDPR è titolare del trattamento di tutti i dati, che confluiscono in essa, ed è responsabile della tutela degli stessi. Da un utilizzo corretto degli smartphone durante l'orario scolastico, a una predisposizione di informative minime per l'impianto di videosorveglianza, fino alla pubblicazione degli esiti degli scrutini risulta fondamentale una corretta applicazione della normativa privacy.
La tecnologia, che pian piano sta modificando il nostro modo di vivere, assume un ruolo fondamentale nella vita scolastica odierna, soprattutto a seguito dei vari Dpcm, conseguenti l'epidemia Covid-19, che hanno costretto migliaia di alunni a continuare la propria attività scolastica dalla propria abitazione utilizzando strumenti tecnologici. Notevole è risultato lo sforzo delle istituzioni scolastiche e universitarie, degli studenti e degli stessi genitori per proseguire l'attività scolastica. Importanti le parole dei due Garanti Privacy, l'uscente Soro e l'entrante Stanzione, che hanno saputo fornire indicazioni utili per un giusto approccio tra l'utilizzo delle nuove tecnologie durante la D.A.D., didattica a distanza, e tutela della privacy.
Così come afferma il Garante Privacy, il Prof. Pasquale Stanzione, in un momento di cambiamento, in cui la tecnologia fa passi da gigante e muta rapidamente, il ruolo della privacy non deve essere quello della rincorsa, bensì, quello della duttilità e della lungimiranza, che consentono un adattamento continuo alla materia da regolare. Solo attraverso un utilizzo così elastico, la privacy saprà sempre adattarsi a un mondo in continuo cambiamento, al fine di una tutela completa e omogenea dei diritti fondamentali.

Coordinamento editoriale:

Gruppo di lavoro *Data Protection Law*

This work is published under a Creative Commons Attribution-NonCommercial-No-Derivatives 4.0 International License (CC BY-NC-ND 4.0). You may freely download it but you must give appropriate credit to the authors of the work and its publisher, you may not use the material for commercial purposes, and you may not distribute the work arising from the transformation of the present work.