UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Tutela penale del diritto alla Privacy. Profili di responsabilità penale del DPO

Federico Vallini

Avvocato

federico@studiolegalevallini.it

Martedì 19 Settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Quali sono le fattispecie di reato attualmente previste a tutela della Privacy

- Il Regolamento europeo 679/2016 non ha previsto le fattispecie penali e relative sanzioni, limitandosi a consentire che gli Stati membri "…*dovrebbero poter stabilire disposizioni relative a sanzioni penali*…"

- Le fattispecie criminose ad assumere maggior rilievo in ambito privacy sono contenute sia all'interno del **codice penale** e del **codice privacy**

CODICE PENALE

Fattispecie che, pur se attengono alla tutela di beni giuridici diversi, sono strettamente connesse alla tutela dei dati personali

- **ART. 615 ter: Accesso abusivo a un sistema informatico o telematico**
- **ART. 615 quinquies: Diffusione di apparechiature, dispositivi o programmi informatici**

  diretti a danneggiare o interrompere un sistema informatico o telematico
- **ART. 640 ter c.p. Frode informatica**
- **ARTT. da 635 bis a 635 quinquies c.p.**

ART. 615 ter c.p. Accesso abusivo a un sistema informatico o telematico

- 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 la reclusione fino a tre anni.
- La pena è della reclusione da uno a cinque anni:
- 1) 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 del sistema;
- 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 3) 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.

ART. 615 ter c.p. Accesso abusivo a un sistema informatico o telematico

- diretta conseguenza dell'evoluzione del settore informatico e rappresenta una delle fattispecie più complesse e pertinenti al tema della privacy, specie se affrontato in un'ottica internazionale, visto il fenomeno sempre più incisivo della pirateria informatica.
- Il bene giuridico oggetto di tutela è la **riservatezza informatica** e la **indisturbata fruizione del sistema informatico** da parte del gestore.

- La norma punisce **due condotte**:

1. l'accesso non autorizzato in un sistema informatico o telematico protetto;
2. il mantenimento in esso contro la volontà de gestore.

- Si configura anche quando il soggetto è abilitato ad accedere al sistema ma vi si introduce per raccogliere dati protetti **per fini estranei** alle ragioni per cui possiede le chiavi di accesso, utilizzando dunque il sistema per finalità diverse da quelle consentite, nonché **a prescindere da una effettiva acquisizione dei dati**.

ART. 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

- Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici[(3)], è punito con la reclusione fino a due anni e con la multa sino a euro 10.329

ART. 615 quinquies c.p. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

- introdotto con la l. 48/2008, che ha ratificato la Convenzione di Budapest
- Il **bene giuridico** oggetto di tutela è la **riservatezza informatica** e la **indisturbata fruizione del sistema informatico da parte del gestore**.
- Si tratta di una delle fattispecie più pericolose e diffuse perché attraverso il ricorso a strumenti tecnici relativamente accessibili a chiunque, è possibile condurre attacchi su scala internazionale. Es. i cd. Ransomware

ART. 640 ter c.p. Frode informatica

- Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.
- La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.
- La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.
- Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età.

ART. 640 ter c.p. Frode informatica

- Le modalità di realizzazione di questa fattispecie illecita sono molteplici: si pensi alla falsificazione o clonazione di carte di pagamento effettuata acquisendo i dati tramite alterazioni dei sistemi di pagamento online o alla cd. "salami techniques", che consiste nella sottrazione illecita e protratta nel tempo di importi ridotti dal proprio conto, resa possibile da programmi creati ad hoc.

- Sotto questa definizione rientra, tra le altre, una delle attività illecite più diffuse: **il phishing**.

Altre fattispecie

- ART. 635 bis c.p. Danneggiamento di informazioni, dati e programmi informatici

- ART. 635 ter c.p. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

- ART. 635 quater c.p. Danneggiamento di sistemi informatici o telematici

- ART. 635 quinquies c.p. Danneggiamento di sistemi informatici o telematici di pubblica utilità

- Tutte «declinazioni» del reato di danneggiamento di cui all'art. 635 c.p.

CODICE PRIVACY

reati previsti e puniti dal d.lgs. 196/2003, per come recentemente novellato dal D.L. 8 ottobre 2021, n. 139

- **ART. 167 - Trattamento illecito di dati**
- **ART. 167 bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**
- **ART. 167 ter, Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**
- **ART. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante**
- **ART. 170 - Inosservanza di provvedimenti del Garante.**
- **ART. 171 - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.**
- **ART. 172 – Pene accessorie**

ART. 167 - Trattamento illecito di dati

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
- 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
- 4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
- 5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
- 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

ART. 167 - Trattamento illecito di dati

- **elementi costitutivi** del reato:
  - anzitutto la necessità che vi sia un **nocumento** per gli interessati (pregiudizio giuridicamente rilevante di qualsiasi natura, patrimoniale e non, cagionato sia alla persona alla quale i dati illecitamente trattati si riferiscono sia a terzi quale conseguenza della condotta illecita (Corte di cassazione, sezione III penale, sentenza 28 marzo 2017 n. 15221).
  - trasferimento di dati all'estero
  - comunicazione e collaborazione fra Garante e Pubblico Ministero
- **Dolo specifico**: la condotta sia posta in essere per generare un profitto per l'agente o altri soggetti ovvero per arrecare un danno all'interessato, destinatario della condotta illecita.

ART. 167 bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

- 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2 ter, 2 sexies e 2 octies, è punito con la reclusione da uno a sei anni.
- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.
- 3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

ART. 167 bis - Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

- **Condotte sanzionate**: da una parte la comunicazione o diffusione che avviene "in violazione degli articoli 2-ter, 2- sexies e 2-octies" e dall'altra quelle che avvengono in casi in cui non vi era stato un preventivo consenso alla comunicazione o diffusione.
- **Dolo specifico**: la finalità di conseguire un profitto o arrecare un danno sono le medesime già descritte all'art. 167;
- **Tutela anticipata**: non è necessario che si realizzi un nocumento per la vittima.
- **Archivio automatizzato**: art. 4, par. 1, n. 6), GDPR stabilisce che archivio è "qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico".

ART. 167 ter - Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.
- 2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

- Se la prima norma puniva la comunicazione e la diffusione degli archivi, in questo caso alle stesse condizioni ne viene sanzionata l'acquisizione (chi riceve le informazioni illecitamente diffuse e le adopera a proprio vantaggio o altrui danno).
- **Dolo specifico**

ART. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

- 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
- 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

ART. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

- **Condotta**: falsità nelle comunicazioni rese al Garante, ma anche l'ostacolo alla regolarità delle verifiche, delle ispezioni, dei procedimenti effettuati dal garante stesso.
- **Dolo generico**
- Dovere di trasparenza e collaborazione con le autorità.
- Fondamentale: presenza di un collegamento diretto e leale fra le autorità di controllo e i titolari del trattamento, comunicazione che viene esercitata in particolare dal D.P.O. (es. **data breach**)
- La norma incriminatrice commentata rappresenta quindi un ulteriore profilo di responsabilità che può coinvolgere in prima persona il **DPO**.

ART. 170 - Inosservanza di provvedimenti del Garante

- 1. Chiunque, non osservando il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2 septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163, arreca un concreto nocumento a uno o più soggetti interessati al trattamento è punito, a querela della persona offesa, con la reclusione da tre mesi a due anni.

Modificato di recente dal D.L. 8 ottobre 2021, n. 139, convertito, con modificazioni, dalla L. 3 dicembre 2021, n. 205

ART. 170 - Inosservanza di provvedimenti del Garante

- Modifica ha introdotto il «concreto nocumento».
- Art. 58 del Regolamento impone "…una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento" destinato ad una realtà specifica; ovvero di una delle misure di garanzie di cui all'art. 2 septies volte ad individuare "le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, misure di minimizzazione, specifiche modalità di accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché eventuali altre misure necessarie a garantire i diritti degli interessati"; nonché i provvedimenti generali di cui all'art. 21 comma I del decreto di armonizzazione.
- DPO non ha poteri di gestione diretta, quindi non potranno essere ipotizzate responsabilità da parte sua in caso di inosservanza ex se dei provvedimenti del Garante.
- Tuttavia, anche dato il suo ruolo di "punto di contatto", egli dovrà dar conto al titolare o al responsabile di ogni iniziativa presa dal Garante che interessi la struttura in cui si trova ad operare come soggetto qualificato e specializzato, con conseguenza che una mancanza da questo punto di vista potrebbe esporlo a un concorso nel reato citato.

ART. 171 - Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

- 1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

- La fattispecie penale punisce tutte quelle violazioni connesse all'impiego di impianti audiovisivi o altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori per esigenze che non siano organizzative e produttive, legate alla sicurezza sul lavoro o alla tutela del patrimonio aziendale, nonché tutte quelle violazioni legate al mancato rispetto della procedura autorizzativa (sindacale o amministrativa) circa l'installazione degli impianti stessi.
- Compromesso tra **tutela della libertà del lavoratore** e **potere di controllo da parte del datore**
- Le nuove tecnologie abbiano esasperato questa **tensione**, mettendo a disposizione strumenti che, in alcuni casi, sono in grado di esercitare un controllo a distanza anche fra paesi diversi.
- Per il DPO è quindi importante saper intervenire sul punto in modo equilibrato, competente e capace di mediazione.

ART. 172 - Pene accessorie

- 1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza, ai sensi dell'articolo 36, secondo e terzo comma, del codice penale.

- Prevede la pubblicazione dei provvedimenti di condanna, ai sensi del secondo e terzo comma dell'art. 36 c.p.
- Si tratta senz'altro di un ulteriore incentivo a evitare di incappare in sanzioni relative alla privacy, considerato che questo avrebbe un costo rilevante anche in termini di reputazione e di immagine.

DPO E RESPONSABILITÀ PENALE

RESPONSABILITÀ PENALE DPO

- Occorre prendere atto che la attuale situazione tecnologica e giuridica non consente, nemmeno laddove siano state dotate effettive misure di prevenzione e sicurezza, di ritenersi al riparo da qualsiasi tipo di rischio.
- Del resto il GDPR fonda la propria strategia di sicurezza sul risk- based-approach, unitamente al principio di accountability, il tutto fungendo da corollario della privacy by design.
- Approccio la cui responsabilità ultima ricade in capo al titolare, tuttavia, trattandosi di attività che richiedono competenze peculiari, il ruolo del D.P.O. diviene **decisivo** nel momento in cui ci si appresta ad affrontare il gravoso impegno di strutturare un'organizzazione complessa in modo da assicurarne la compliance.
- L'importanza del ruolo del D.P.O. consente di ipotizzare la sussistenza di responsabilità in capo allo stesso anche dal punto di vista penalistico, considerato che, ai sensi dell'art. 39, par. 2 del regolamento, egli è chiamato a tenere in debita considerazione i fattori di rischio che si possono presentare nell'espletamento dei suoi incarichi (in particolare DPIA e DATA BREACH).

RESPONSABILITÀ PENALE DPO

- Ipotesi diretta: es. Data Breach
- Concorso nel reato ex Art. 110 c.p. *Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti*.
- DPO - RSPP
- Titolare di una posizione di garanzia ex art. 40 c.p. *Rapporto di causalità – Nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende la esistenza del reato, non è conseguenza della sua azione od omissione. 2.* ***Non impedire un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo****.*
- **POSIZIONE DI GARANZIA** ovvero l'obbligo giuridico di impedire l'evento.

RESPONSABILITÀ PENALE - DPIA

- l'onere di riconoscere la necessità di provvedere alla D.P.I.A. e di farvi fronte efficacemente spetta al titolare, che però ha l'obbligo di consultarsi con il D.P.O., ai sensi del par. 2 dell'art. 35. Il compito di "sorvegliante" dell'osservanza del regolamento in questo caso si manifesta nella necessità di fornire un parere a richiesta del titolare.
- il D.P.O. è chiamato a fare in modo che vengano rispettate le disposizioni e i diritti previsti nel GDPR e nelle altre normative dell'Unione in materia di tutela dei dati personali.
- Se un determinato trattamento viene posto in essere mettendo in pericolo la sicurezza di tali diritti e disposizioni e da ciò derivino conseguenze tali da integrare una fattispecie di reato, il D.P.O. il quale non ha segnalato i fattori di rischio in fase di D.P.I.A. (eventualmente indicando al titolare la contrarietà del trattamento alle disposizioni normative ovvero suggerendo il ricorso alla consultazione preventiva ex art. 34 del regolamento) ovvero ancora ha dato esplicitamente il suo avallo a soluzioni non conformi al regolamento, può essere ipotizzabile una responsabilità penale, stante la configurabilità di una posizione di garanzia che gli impone non già di compiere azioni di gestione che, come detto, non gli competono, bensì di assicurarsi che il titolare sia reso consapevole di tutte quelle situazioni che costituiscono un vulnus alla corretta applicazione della normativa e quindi alla sicurezza e integrità dei dati

RESPONSABILITÀ PENALE – DATA BREACH

- Anche qui il DPO riveste un ruolo importante perché in virtù della sua specializzazione, dovrà essere in grado di identificare quali siano quelle violazioni che rispondono ai criteri individuati dal regolamento come base normativa dell'obbligo di notifica all'autorità garante
- è chiamato ad essere il punto di contatto fra l'autorità garante e la struttura per quel che riguarda la gestione della vicenda, come da articolo 33, par. 3 lett b) e 39, par. 1, lett. e) del regolamento
- Quindi è fondamentale che da parte sua vi sia una piena e leale collaborazione con l'autorità garante, cui deve comunicare le azioni e le eventuali omissioni commesse all'interno della struttura in cui opera.
- Qualora si comportasse diversamente si può ipotizzare che possa incorrere nelle fattispecie di reato di cui agli artt. 168 e 170 del d.lgs. 196/2003.

CONCLUSIONI

- La conoscenza di questi aspetti relativi alla materia penale deve essere presente ai soggetti interessati e, in particolare, al D.P.O. perché, nello svolgere le proprie funzioni di **consulenza, assistenza e sorveglianza**, egli dovrà certamente prestare attenzione ai **profili di rischio** sui quali possono innestarsi le principali fattispecie di reato in ambito di privacy e, conseguentemente, rilevare e segnalare eventuali aspetti critici presenti nella struttura affidata alla sua attenzione.

GRAZIE

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection