UNIVERSITA' CATTOLICA DEL SACRO CUORE DI MILANO

Master Universitario di II livello
in
Diritto Penale dell'Impresa

IMPRESA, CRIMINALITA' INFORMATICA E TUTELA DEI DATI

Dott.ssa Claudia LOIACONO

Anno Accademico 2017/2018

INDICE

IMPRESA, CRIMINALITA' INFORMATICA E TUTELA DEI DATI

Pag.

Introduzione

Capitolo I

CRIMINALITA' INFORMATICA

1. Progressiva emersione della categoria dei reati informatici……..4

2. Bene tutelato……..6

Capitolo II

CYBERCRIMES E RESPONSABILITA' DEGLI ENTI

1. Responsabilità amministrativa degli enti e reati informatici ……..……..….9

2. L'art. 24 bis del decreto legislativo 231 del 2001……..10

2.1 Delitti informatici presupposto del d.lgs. 231/2001…….……..11

2.1.1 Reato di accesso abusivo ad un sistema informatico o telematico…….12

Capitolo III

TRATTAMENTO DEI DATI PERSONALI E RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI ALLA LUCE DEL D. LGS. N. 101/2018

1. Riservatezza, privacy e diritto alla protezione dei dati personali: differenze.……16

2. Illecito trattamento dei dati personali e responsabilità degli enti…….……..19

3. Modelli organizzativi *privacy* e 231……..21

Conclusioni 25

Bibliografia

Introduzione

Il nuovo millennio ha visto un incessante sviluppo tecnologico che, se da un lato ha dato vita a opportunità di progresso sul piano sociale, economico e culturale, dall'altro ha costituito un terreno fertile per nuove tipologie e modalità di comportamenti penalmente rilevanti.

Infatti, con l'espansione di Internet e dei nuovi prodotti tecnologici sono incrementate le possibilità di aggredire, oltre i beni giuridici tradizionali (onore e reputazione, patrimonio, proprietà intellettuale, ecc.), anche interessi totalmente nuovi, quali la protezione di dati personali, la riservatezza informatica e l'integrità, anch'essi meritevoli di tutela penale[1].

Nonostante compaia in varie fonti sovranazionali ed europee[2], la "criminalità informatica" non rappresenta una categoria definita giuridicamente, né esiste una definizione riconosciuta a livello internazionale di "*cybercrime*" o "*computer crime*"[3].

Attualmente, si ritiene che rientrino nel concetto di "criminalità informatica" quei fatti criminosi che possono essere commessi attraverso la rete o nel *cyberspace*, ovvero quello spazio virtuale che rende difficoltosa sia la localizzazione delle risorse e la loro raggiungibilità, da parte dell'utente, da ogni luogo e distanza, sia la collocazione temporale delle attività che possono essere progettate e svolte attraverso operazioni automatizzate

[1] Sulla nascita e lo sviluppo di questi nuovi interessi v. I. Salvadori, *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* in L. PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 125 ss., p. 149 ss; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati, in Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss., p. 70 ss.

[2] Convenzione *Cybercrime* adottata a Budapest il 23 novembre 2001; la direttiva 95/46/CE sulla tutela dei dati personali, nonché le direttive successive adottate in questo settore; le direttive in materia di protezione dei diritti d'autore e, in particolare, la direttiva 2001/29/CE; la direttiva 2000/31/CE sul commercio elettronico, le decisioni quadro contro gli attacchi informatici (2005/222/GAI), contro lo sfruttamento sessuale di minori e la pedopornografia (2004/68/GAI), contro il terrorismo (2002/475/GAI, parzialmente riformata dalla decisione 2008/929/GAI); sul piano processuale vedi quelle sul mandato d'arresto europeo (2002/584/GAI) e sull'applicazione del principio del reciproco riconoscimento delle decisioni di confisca (2006/783/GAI), che includono la "criminalità informatica" nelle liste dei reati per cui si prescinde, in conformità col principio del mutuo riconoscimento, dal requisito della doppia incriminazione per l'esecuzione diretta dei provvedimenti emessi dall'autorità giudiziaria dello Stato richiedente. V. L. Picotti, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *Riv. Trim. dir. Pen. ec.,* 4, 2011, p. 827 e ss.

[3] G. VACIAGO, *Internet e i crimini informatici*, in M. L. PICCINI, G. VACIAGO*, Computer crime: casi pratici e metodologie investigative dei reati informatici*, Bergamo, Moretti&Vitali, 2008, pp. 12 ss.; M. F. WEISMANN, *Internation Cybercrime: Recent Developments in the Law*, in R.D. Clifford (ed.), *Cybercrime*, 2011, p. 257.

dall'utente, senza la necessaria presenza fisica della persona umana davanti allo schermo di un computer.

Si tratta di quei comportamenti lesivi di interessi penalmente rilevanti che sono riconducibili ai cd. "reati informatici". Occorre, però, fare una distinzione[4] tra reati informatici in senso stretto[5], caratterizzati da elementi di tipizzazione connessi a procedimenti di automatizzazione di dati o informazioni, e cioè in cui la connessione in rete e l'utilizzo del *cyberspace* ne sono il fondamento, e reati informatici in senso lato[6], in cui rientrano tutte quelle fattispecie che possono essere applicate a fatti che non abbiano le caratteristiche proprie della tecnologia, ma che possono essere commessi attraverso l'utilizzo della stesso, della rete o comunque nel *cyberspace*.

La prima categoria si connota per un nuovo oggetto passivo su cui la condotta va a cadere (i programmi, le informazioni, i dati o altri "prodotti" informatici o digitali) oppure dal fatto che il computer ed i prodotti informatici in genere costituiscono lo strumento tipico di realizzazione del fatto criminoso.

Nella seconda categoria, invece, rientrano quei comportamenti criminosi che sono qualificati come illeciti caratterizzati dal mezzo di aggressione, che sarebbero realizzabili o concepibili a prescindere dall'informatica e dalla rete.

Pertanto, essendo vietato il ricorso all'analogia dal principio di legalità *ex* art. 25 comma 2 cost., per colmare quelle lacune che sono emerse sempre più frequentemente nella

[4] F. R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *dir. Pen. proc*., 2009, p. 639 e ss.; R. FLOR, *Lotta alla "criminalità organizzata" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *dirittopenalecontemporaneo.it*.

[5] V. L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *riv. Trim. dir. Pen. ec*., 4, 2011, p. 827 e ss. Si pensi, nell'ordinamento italiano, alla frode informatica (art. 640 ter. C.p.) o all'accesso abusivo a sistemi informatici (art. 615 ter. C.p.).

[6] Si consideri la truffa (art. 640 c.p.), che può essere commessa attraverso l'invio di email ingannevoli che inducono in errore il destinatario determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti online .Oppure la diffamazione online, o le forme di manifestazione o diffusione del pensiero o di contenuti illeciti, quale la rivelazione o agevolazione "in qualsiasi modo" della conoscenza, da parte di terzi non legittimati, di una notizia che debba rimanere segreta.

prassi, è dovuto intervenire il legislatore. Sono state, infatti, introdotte nuove fattispecie incriminatrici ed è stato esteso l'ambito di altre già esistenti.

È nato, così, il "diritto penale dell'informatica", che, però, non essendo stato il frutto di un'idea costitutiva, ma, anzi, essendo stato costruito attraverso l'accorpamento di materiali diversi, risulta essere privo di un organico disegno sistematico[7].

La svolta è stata data dalla legge 23 dicembre 1993 n. 547[8], la quale ha cercato di fornire una risposta alle esigenze di contrastare la criminalità informatica, integrando e modificando il codice penale e il codice di procedura penale. Tuttavia, questo intervento normativo è stato realizzato non attraverso l'inserimento delle nuove disposizioni in un titolo autonomo, bensì inserendole nei diversi titoli già esistenti.

[7] «Ad esempio, nel codice penale compare il reato di frode informatica (art. 640 *ter* c.p.) tra i delitti contro il patrimonio e sono distribuite tra i delitti contro l'inviolabilità del domicilio e contro l'inviolabilità dei segreti le fattispecie introdotte ex novo nel 1993, che forse avrebbero meritato una collocazione autonoma. Altre fattispecie, invece, compaiono in leggi speciali: i reati di indebito utilizzo di carte di credito o bancomat (l. n. 197 del 1991) e quelli relativi all'adeguamento a convenzioni internazionali, contenuti nella legge sul diritto d'autore (l. n. 633 del 1941), nei decreti legislativi sulla protezione dei dati personali (d.lgs. 196 del 2003) e sul commercio elettronico (d.lgs. n. 70 del 2003)».Vedi L. Picotti, *Internet e diritto penale: il quadro alla luce dell'armonizzazione internazionale*, in *diritto dell'internet*, 2, 2005, p. 189 e ss.; F. R. Fulvi, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *dir. Pen. proc*., 2009, p. 639 e ss.

[8] Sulla l. 547/93 v. CUOMO - RAZZANTE*, La nuova disciplina dei reati informatici*, Torino, 2009, p. 29 e ss.; RESTA, *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica del diritto, giur. Merito*, 11, 2006, p. 102 e ss.; SOLA, *Prime considerazioni in merito alla legge 547/1993*, in *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Bologna, 1995, p. 5 e ss.

CAPITOLO I

CRIMINALITA' INFORMATICA

SOMMARIO:

1. Progressiva emersione della categoria dei reati informatici. – **2.** Bene tutelato.

---

1. Progressiva emersione della categoria dei reati informatici.

È stata la Raccomandazione del Consiglio d'Europa del 13 settembre 1989 sulla criminalità informatica a dare un *input* per il rafforzamento delle politiche legislative in materia di reati informatici, sulla base dei risultati del rapporto elaborato dal Comitato Europeo per i problemi criminali.

All'interno della Raccomandazione era stata elaborata una lista minima in cui erano indicate le principali condotte della criminalità informatica: il falso in documenti informatici, la frode informatica, il sabotaggio informatico, il danneggiamento di dati, l'intercettazione di comunicazioni informatiche, l'accesso abusivo a un sistema informatico e la violazione dei diritti di esclusiva su un programma informatico protetto (che costituivano le nuove opere dell'ingegno nate dall'uso della tecnologia informatica).

Vi era, inoltre, una lista facoltativa di condotte, per le quali era stata lasciata discrezionalità ai singoli legislatori nazionali sull'opportunità di sanzionarle o meno[9].

Dato, poi, il rapido sviluppo della tecnologia, tali reati avevano raggiunto una nuova dimensione, motivo per cui il Consiglio d'Europa è giunto all'elaborazione della Convenzione sulla criminalità informatica, cd. *Cybercrime*, stipulata a Budapest il 23 novembre 2001 ed entrata in vigore nel 2004.

[9] Si trattava dell'alterazione di dati e/o programmi, dello spionaggio informatico, dell'utilizzazione non autorizzata di un programma informatico protetto.

Questa rappresentava uno strumento più incisivo e vincolante rispetto alla Raccomandazione, posto che mirava ad armonizzare i vari ordinamenti penali sia sul piano sostanziale che processuale.

La Convenzione, infatti, indica un oggetto necessario di incriminazione individuandolo nelle condotte di abuso che precedentemente erano ricondotte alla nozione di reato informatico, facendo una distinzione, però, a seconda che lo strumento informatico fosse oggetto o strumento di aggressione[10].

In un primo gruppo rientrano le offese arrecate alla riservatezza, all'integrità e alla disponibilità dei dati e dei sistemi informatici (accesso abusivo al sistema, intercettazione di comunicazioni informatiche, danneggiamento dei dati, sabotaggio informatico).

Il secondo gruppo è caratterizzato da quelle condotte in cui il sistema informatico rappresenta lo strumento o il mezzo per la commissione dei tradizionali reati di falso e di truffa, ovvero la falsificazione di dati informatici e la frode informatica, in quanto *computer-related offences*.

Vi è, poi, un gruppo in cui rientrano le violazioni del diritto d'autore sulle opere dell'ingegno ed una serie di condotte riguardanti la pornografia infantile, caratterizzate dall'utilizzo del sistema informatico della commissione del reato.

Il Consiglio d'Europa, pertanto, richiede agli Stati di predisporre delle sanzioni effettive, dissuasive e proporzionate per questi reati, indicando, inoltre, come necessaria la previsione di una concorrente responsabilità anche per le persone giuridiche nel caso in cui il reato fosse stato commesso nel loro interesse da un soggetto dotato di poteri di rappresentanza, gestione o controllo al suo interno, o che fosse stato reso possibile dalla mancanza di controllo o sorveglianza su un soggetto ad essi sottoposto[11].

---

[10] C. PECORELLA, *Reati informatici*, in *Enc. Dir.,* 2017, p. 707 e ss.

[11] Nel nostro ordinamento questa esigenza è stata soddisfatta con la l. 18 marzo 2008 n.48 che, attraverso l'inserimento dell'art. 24 bis nel d.lgs. 231/2001 ha esteso la responsabilità degli enti, originariamente prevista solo per le ipotesi di frode informatica in danno dello Stato o di altri enti pubblici (art. 24), a quasi tutti i reati

Nell'ordinamento italiano, alla luce di quanto impartito a livello internazionale, si possono individuare quattro macroclassi di delitti informatici per i quali il legislatore ha creato disposizioni *ad hoc*, per lo più inserendole nel codice penale a completamento della tutela già assicurata, rispetto alle modalità di offesa tradizionali, ai diversi beni aggrediti.

Si possono distinguere, quindi, le aggressioni alla riservatezza dei dati e delle comunicazioni informatiche, le aggressioni all'integrità dei dati e dei sistemi, le frodi informatiche e la falsificazione di documenti informatici.

Queste tipologie di aggressione, dopo la Convenzione di Budapest, vengono indicate con il nome di "reati informatici in senso stretto" per distinguerle dalle altre forme di criminalità informatica che sono per lo più represse attraverso disposizioni penali di carattere meramente sanzionatorio[12].

2. Bene tutelato.

È pacifico che il diritto penale ha come compito principale la tutela di beni giuridici e la prevenzione delle condotte offensive, pertanto l'introduzione di nuove norme deve essere giustificata da questa finalità.

Un sistema giuridico per essere armonico quindi deve contenere distinte categorie di tutela, la loro graduazione e la riduzione al minimo della possibilità di duplicazione o di contraddittorietà dei precetti[13]. Pertanto, occorre valutare se, applicando questi concetti, sia possibile ricostituire in unità le varie norme in materia di diritto penale dell'informatica sparse

---

informatici presenti nel codice penale. Sul tema v. BELLUTA, *Cybercrime e responsabilità degli enti,* in *Sistema penale e criminalità informatica* a cura di LUPARIA, Milano, 2009, p. 83 e ss.

[12] E' il caso delle violazioni dei diritti di esclusiva dell'autore di nuove opere dell'ingegno nate con l'informatica, così come delle aggressioni alla privacy derivanti dalla violazione delle disposizioni che disciplinano la raccolta e l'utilizzo di dati personali. A questo diverso ambito appartengono anche quei reati la cui dimensione informatica è del tutto eventuale e dipende dall'impiego di un sistema informatico per la loro realizzazione. Questo è il caso delle *content-related offences* così come qualsiasi reato "tradizionale" commesso in rete. V. C. PECORELLA, *Reati informatici*, in *Enc. Dir.,* 2017, p. 707 e ss.

[13] F. R. FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *dir. Pen. proc*., 2009, p. 639 e ss.; F. Modugno, *Ordinamento giuridico*, in *Enc. Dir*., XXX,1980, p. 678 e ss.

nell'ordinamento. È essenziale quindi identificare il bene giuridico di categoria che permetta di dare un'armonia concettuale ai vari reati informatici.

Le nuove norme sono in parte il frutto di esigenze di tutela derivanti dalle emergenze occasionali ed in parte sono attuative di convenzioni, direttive e raccomandazioni di fonte europea e sovranazionale, da cui sono derivati una serie di interventi settoriali[14].

È solo con la legge 23 dicembre 1993 n. 547 che si è cercato di dare un disegno unitario, con l'integrazione e la modificazione di fattispecie che potessero adattarsi il più possibile al tessuto normativo preesistente.

Tre sono le modalità di intervento con cui il legislatore ha agito. Innanzitutto ha voluto dare attuazione all'interno del codice penale le Raccomandazioni del Consiglio di Europa in materia di criminalità informatica combinando le esigenze di tutela emerse in sede nazionale, con l'introduzione di nuovi delitti[15]. Il legislatore è intervenuto, poi, nel settore del diritto d'autore, introducendo nuove fattispecie incriminatrici con l'intento di adeguare la disciplina extrapenale alle nuove tecnologie. Ed infine, con riferimento al settore del trattamento dei dati personali, ha dato vita ad una specie di "microsistema" che include una serie di precetti di natura amministrativa e civile, provvedimenti del Garante, rispetto alle quali le disposizioni penali hanno natura meramente sanzionatoria.

Pertanto, mentre nel codice penale si è intervenuti con delitti che risultano essere "autonomi", contenenti precetti descrittivi assimilati il più possibile a quelli delle fattispecie comuni cui sono affiancati[16], nelle leggi penali speciali, le disposizioni penali hanno

---

[14] Vedi L. PICOTTI, *Internet e diritto penale: il quadro alla luce dell'armonizzazione internazionale*, in *diritto dell'internet*, 2, 2005, p. 189 e ss..

[15] La novella è stata completata dalla successiva legge "contro la pedofilia" in data 3 agosto 1998 n. 269 che ha introdotto nel codice, fra gli altri, il delitto di diffusione di materiale pedopornografico "anche per via telematica".

[16] Si pensi, ad esempio, all'art. 491-*bis* c.p., rubricato «Documenti informatici», volto alla protezione della c.d. fede pubblica documentale, poiché estende la tutela prevista dalle norme del capo III del Titolo VII del libro II del c.p. al documento informati- co privato o pubblico; agli artt. 616, 621, 623 *bis* c.p., rubricati «Violazione, sottrazione e soppressione di corrispondenza», «Rivelazione del contenuto di documenti segreti» e «Altre comunicazioni e conversazioni», che estendono la tutela contenuta nel- le relative fattispecie rispettivamente alla corrispondenza informatica o telematica, al documento informatico e a qualunque altra trasmissione a distanza di

esclusivamente la funzione di sanzionare le violazioni dei precetti extrapenali che le regolano[17].

Alla luce di ciò, nelle fattispecie codicistiche, sembra più agevole individuare i beni giuridici tutelati, distinguendosi, da quelli simili già esistenti a cui sono affiancati, per le nuove modalità di lesione o i diversi oggetti passivi su cui ricadono le condotte delittuose, mentre negli altri reati informatici, in cui la disposizione penale funge da mera sanzione, rinviando per il precetto alle relative discipline extrapenali, non è facile individuare l'oggetto di tutela.

---

suoni, immagini o altri dati; all'art. 640-*ter*, c.p., rubricato «Frode informatica», modellata sul paradigma della truffa comune di cui all'art. 640 c.p. e volta alla tutela del patrimonio. Per un dettagliato esame delle tecniche di formulazione normativa utilizzate dal legislatore in riferimento ai reati informatici si rinvia a L. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, p. 191 e ss.

[17] Si pensi, ad esempio, all'art. 167 del d.lgs. n. 196 del 2003, che sanziona il trattamento illecito dei dati, consistente nel fatto di procedere alle varie attività rientranti nel concetto generale di «trattamento» (definito dall'art. 4, lett. a) del d.lgs n. 196/03) in violazione dei precetti contenuti negli articoli 18 e 19 (sui principi regolatori applicabili al trattamento dei dati da parte di soggetti pubblici), 23 (sul consenso dell'interessato), 123, 126 e 130 ovvero in applicazione dell'art. 129 (norme che attengono al settore della telefonia e delle «comunicazioni elettroniche»); all'art 170 del d.lgs. n. 196 del 2003, che punisce l'inosservanza dei provvedimenti adottati dal Garante ai sensi degli artt. 26, secondo comma, 90, 143, primo comma, lett. c) e 150, primo e secondo comma.

CAPITOLO II

CYBERCRIMES E RESPONSABILITA' DEGLI ENTI

SOMMARIO:

1. Responsabilità amministrativa degli enti e reati informatici. – **2.** L'art. 24 *bis* del decreto legislativo 231 del 2001. – **2.1** Delitti informatici presupposto del d.lgs. 231/2001. – **2.1.1** Reato di accesso abusivo ad un sistema informatico o telematico

---

1. Responsabilità amministrativa degli enti e reati informatici.

La legge del 18 marzo 2008 n. 48 di ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica ha inciso sulle strategie aziendali in materia di *cybercrime*. Infatti, l'art. 7 della legge ha esteso la responsabilità amministrativa dell'ente per la maggior parte dei reati informatici[18].

Per molto tempo le aziende, non solo, non si sono preoccupate di tutelarsi dalla commissione di reati informatici al loro interno ma, anche, evitavano di denunciare il reato. La denuncia avrebbe causato una pubblicità negativa per l'azienda mettendo in risalto la vulnerabilità dei sistemi, ed inoltre, all'epoca, non esisteva ancora una normativa sulla criminalità informatica, pertanto i procedimenti penali che si fossero instaurati si sarebbero conclusi quasi sicuramente con un'archiviazione[19].

Oggi, con l'art. 7 della legge di ratifica della Convenzione di Budapest, è prevista la responsabilità amministrativa delle persone giuridiche per i reati informatici commessi da un

[18] Per una dettagliata analisi della L. 48/2008 e degli effetti prodotti sull'ordinamento giuridico interno dalla sua introduzione: L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. Pen. proc.,* 2008, 6, p. 700 e ss.; F. RESTA, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura*, in *Giurisprudenza di merito*, 2008, 9, p. 2147 e ss.
[19] P. GALDIERI, in *Interlex*, n.376, 26 giugno 2008.

vertice o da un dipendente dell'azienda quando ciò avvenga nel suo interesse o abbia apportato alla stessa un vantaggio[20].

Questo nuovo scenario mette l'azienda nelle condizioni di dover adottare delle misure preventive idonee non solo ad impedire che vengano commessi reati informatici al suo interno ma anche per escludere una responsabilità della stessa nei casi in cui le misure adottate non siano state capaci di evitare la commissione dei reati.

2.1 L'art. 24 bis del decreto legislativo 8 giugno 2001, n. 231

Occorre, dapprima, però, evidenziare come tale intervento normativo non sia privo di aporie.

Già prima del 2008 il d.lgs. 231/2001 conteneva, tra le fattispecie delittuose, delle ipotesi di natura informatica, e cioè il delitto di frode informatica aggravata (ai danni dello Stato o altro ente pubblico) *ex* art. 640 *ter* c.p., prevista dall'art. 24 del decreto, ed il reato rubricato pornografia virtuale *ex* art. 600 *quater* co 1 c.p., previsto, invece, dall'art. 25 *quinquies* del decreto[21]. Pertanto, l'aver creato una disposizione autonoma ulteriore relativa ai delitti informatici è sintomo di una disomogeneità del complesso normativo, in quanto sarebbe stata auspicabile una fattispecie unitaria[22].

---

[20] Per un commento analitico circa l'art. 24 bis si segnalano in dottrina: C. SANTORIELLO - G. DEZZANI - P. DAL CHECCO, *Delitti informatici e trattamento illecito di dati*, in M. LEVIS - A. PERINI (a cura di), Zanichelli, 2014, pp. 461-483; G. DEZZANI - S. RICCI, *Reati informatici e responsabilità amministrativa dell'ente*, in G. CASSANO - G. SCORZA - G. VACIAGO, *Diritto dell'internet. Manuale operativo.* Casi, legislazione, giurisprudenza, Cedam, 2012, pp. 619-636; S. CRIMI, *Commento all'art. 24 bis d.lgs. 231/2001*, pp.306-313, in A. CADOPPI - G. GARUTI - P. VENEZIANI, *Enti e responsabilità da reato*, Utet 2010; F. BOEZIO - G. BRUSTIA, *I crimini informatici*, in S. DI GUARDO - P. MAGGIOLINI - N. PATRIGNANI, *Etica e responsabilità sociale delle tecnologie dell'informazione*, Vol. I, Franco Angeli, 2010, pp. 261-310; MASSIMO CARDUCCI, *La responsabilità delle persone giuridiche e i crimini informatici*, pp. 299-317.

[21] Così H. BELLUTA, *Cybercrime e responsabilità degli enti* p. 87, in L. Luparia, *Sistema penale e criminalità informatica*, 2009; M. CARDUCCI, *La responsabilità delle persone giuridiche e i crimini informatici*, p. 306.

[22] Così G. MORGANTE, sub. art. 7, in *Commento articolo per articolo alla l. 18/3/2008, n. 48*, in *Legisl. pen.*, 2008, p. 279 .

Ulteriore considerazione riguarda la rubrica dell'articolo in esame, posto che recita "Delitti informatici e trattamento illecito di dati", il che sembra fare riferimento all'inclusione nella norma della disciplina non solo dei reati informatici, ma anche degli illeciti contenuti nel d.lgs. 196/2003 (cd. Codice Privacy)[23]. In realtà, però, non vi è traccia di questi delitti nell'art. 24 bis, né sarebbe possibile un'estensione della norma in esame a questi reati in quanto contrasterebbe col principio di tassatività.

2.1 Delitti informatici presupposto del d.lgs. 231/2001.

Passando ad analizzare il testo di legge, si può notare come la norma preveda che, in caso di commissione di un reato informatico, l'ente potrà essere sanzionato non solo con l'esborso di ingenti somme di denaro, ma anche con le interdizioni previste dall'art. 9 comma 2 lett. a), b) ed e) del d.lgs. 231/2001[24].

L'art. 24 *bis*[25], al primo comma, prevede una sanzione pecuniaria che va da un minimo di 100 ad un massimo di 500 quote in caso di commissione dei delitti di: accesso abusivo a sistema informatico (art. 615 *ter* c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 *quater* c.p.), installazione di

[23] S. BELTRANI, *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *La responsabilità amministrativa delle società e degli enti*, n. 4. 2008, p. 24 e ss.

[24] Per una panoramica complessiva su questi reati si veda C. SANTORIELLO, *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti, in La responsabilità amministrativa delle società e degli enti,* n. 1, 2011, pp. 211 ss.

[25] «Art. 24-*bis*. - *(Delitti informatici e trattamento illecito di dati). –*
1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)»

apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 *quinquies* c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635 *bis* c.p.), danneggiamento di informazioni, dati e programmi utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 *ter* c.p.), danneggiamento di sistemi informatici o telematici (art. 635 *quater* c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 *quinquies* c.p.).

2.1.1 Reato di accesso abusivo ad un sistema informatico o telematico[26]

I maggiori rischi in tema di responsabilità delle organizzazioni per delitti informatici riguardano il reato di accesso abusivo ai sistemi informatici o telematici *ex* art. 615 *ter* c.p. Questa norma punisce sia l'introduzione abusiva di un soggetto all'interno di un sistema informatico o telematico che sia protetto da misure di sicurezza, sia la permanenza, in un sistema protetto, contro la volontà espressa o tacita del titolare dello *ius exlcludendi*[27].

Pertanto, vengono sanzionate non solo le condotte che tipicamente sono proprie degli *hacker* esperti ed esterni, ma anche quelle che sono poste in essere da dipendenti o collaboratori. Infatti, un soggetto potrebbe avere l'autorizzazione ad accedere al sistema ed a

---

[26] Art. 615 *ter* c.p.: *«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».

[27] R.FLOR, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reawto e bene giuridico protetto,* in *Dir. Pen. proc.,* 1, 2008, p. 106 e ss.

superare legittimamente le misure di sicurezza, ma la sua condotta diventerebbe punibile nel momento in cui dovesse permanere nel sistema oltre i limiti posti dal titolare al momento dell'autorizzazione dell'accesso.

Elemento costitutivo della fattispecie, però, è la presenza delle misure di sicurezza, in quanto se non ci fossero non sarebbe esclusa la libera disponibilità dei dati (al cui accesso non si è autorizzati). Infatti, il legislatore vuole tutelare il diritto di uno specifico soggetto che abbia dimostrato, però, con la predisposizione di mezzi di protezione logici e fisici, di voler riservare l'accesso o la permanenza nel sistema solo alle persone da lui autorizzate. Pertanto, la presenza di misure di sicurezza è funzionale non solo alla selezione di sistemi informatici meritevoli di tutela, ma anche a manifestare la volontà del titolare dello *spatium operandi et deliberandi* di escludere soggetti non autorizzati[28].

Questo elemento ha creato problemi interpretativi in dottrina e giurisprudenza, posto che il legislatore non ha specificato né la natura né l'intensità delle misure di sicurezza[29].

Si ritiene che le protezioni abbiano certamente una funzione costitutiva della fattispecie, ma non è la loro violazione a costituire la volontà di aggredire da parte del reo o il momento in cui avviene la lesione del bene protetto[30]. In altre parole, si ritiene configurata la condotta di accesso abusivo ad un sistema informatico o telematico con la inosservanza della volontà del titolare dell'accesso e non con la violazione delle "misure di sicurezza".

Le due condotte sanzionate dalla norma ("*chiunque abusivamente si introduce…ovvero vi si mantiene"*) sono formulate in modo alternativo e non potrebbe essere diversamente, posto che l'intrusione abusiva può realizzarsi solo a seguito di un accesso

---

[28] R.FLOR, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in *Dir. Pen. proc.,* 1, 2008, p. 106 e ss.
[29] PESTELLI, *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico*, in *Cass. Pen*., 2012, 6, p. 2330.
[30] V. SPAGNOLETTI, *Art. 615* ter *c.p.: il domicilio informatico tra profili dogmatici e problemi applicativi*, in *Giur. merito*., 2004, 181 e ss.

illecito, viceversa, la permanenza non autorizzata può realizzarsi solo a seguito di un accesso lecito.

Per quanto riguarda il bene giuridico tutelato si ritiene sia il domicilio informatico, ovvero il diritto disporre, godere e controllare le informazioni, i dati e i sistemi in capo al titolare dello "spazio informatico"[31].

Occorre distinguere, però, il reato in esame dalla più generale fattispecie di violazione di domicilio disciplinata dall'art. 614 c.p. Infatti, ai fini della configurabilità del reato di accesso abusivo a sistemi informatici o telematici si fa riferimento anche a misure di sicurezza "fisiche", ma occorre che si riferiscano alle modalità di utilizzo di un sistema. Pertanto, non può ritenersi sufficiente, ad es., una chiusura dei locali dove si trova il sistema, priva di altre specifiche misure di protezione, in quanto in questo caso l'ingresso abusivo realizzerebbe la condotta di cui all'art. 614 c.p. qualora si fossero realizzati i relativi presupposti di legge[32]. Si pensi, ad esempio, alle misure previste all'interno di un'azienda che richiedano un *badge* per accedere nell'area dove si trovano i *computer,* solo in questo caso le misure di sicurezza possono ritenersi espressamente poste per impedire un uso abusivo del sistema.

L'accesso abusivo ad un sistema informatico, dal punto di vista soggettivo, richiede la sussistenza del dolo generico, ovvero è necessario che il soggetto sia consapevole di introdursi o di permanere all'interno del sistema protetto da misure di sicurezza contro la volontà del titolare dello *ius excludendi alios*. Pertanto, non rileva il fine a cui è diretto

[31] L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 21 e ss.; G. PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 1 e ss. e 38 e ss.; C. PECORELLA, *Il diritto penale dell'informatica*, Padova, rist., 2006, in particolare 306 e ss.
[32] G. AMATO - V.S. DESTITO - G.DEZZANI - C. SANTORIELLO, *I reati informatici*, 2010, p. 72.

l'accesso abusivo o la permanenza nel sistema, né il motivo per cui il soggetto pone in essere la condotta[33].

[33] G. PESTELLI, *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico,* in *Cass. pen.,* fasc. 6, 2012, p. 2320B.

CAPITOLO III

TRATTAMENTO DEI DATI PERSONALI E RESPONSABILITA' AMMINISTRATIVA DEGLI ENTI ALLA LUCE DEL D. LGS. N. 101/2018

SOMMARIO:

1. Riservatezza, privacy e diritto alla protezione dei dati personali: differenze.– **2.** Illecito trattamento dei dati personali e responsabilità degli enti. – **3.** Modelli organizzativi *privacy* e 231.

---

1. Riservatezza, privacy e diritto alla protezione dei dati personali: differenze.

Tra gli interessi venuti in rilievo con l'evoluzione tecnologica e cibernetica[34] vanno indicati anche la riservatezza, la privacy e il diritto alla protezione dei dati personali, nozioni simili ma non esattamente coincidenti.

La riservatezza può essere intesa come il diritto a una "vita intima"[35] riconducibile al catalogo dei diritti della personalità[36]. Questa, con l'intensificarsi delle attività nel *Cyberspace*, ha trovato una sua declinazione nella "riservatezza informatica" che viene identificata come «potestà di escludere terzi e di essere garantiti contro intrusioni indesiderate ed interferenze potenzialmente dannose o comunque non consentite, per salvaguardare un

[34] Sul punto v. F. MORALES PRATS, *Presupposti politico-criminali per una tutela pena della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo),* in *dir. Inf*., p. 369 ss.

[35] M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *jusonline*, n. 1, 2017, p. 218 e ss.

[36] Viene definita come «modo di essere della persona il quale consiste nella esclusione dalla altrui conoscenza di quanto ha riferimento alla persona medesima» da P. RESCIGNO, *Il diritto ad essere lasciati soli,* in *Synteleia per Vincenzo Arangio Ruis,* Napoli, 1964, p. 494. Sul punto anche R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003; Z.ZENCOVICH, *I diritti della personalità dopo la legge sulla tutela dei dati personali,* in *Studium iuris,* 1997, p 467 ss.; F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* in *Riv. It.dir. proc. Pen.,* p. 1079 ss.; B. FRANCESCHELLI, *Il diritto alla riservatezza,* Napoli, 1960;

proprio "spazio informatico" libero, autonomo e sicuro, in cui possa svolgersi senza impedimenti la propria personalità, che opera tramite relazioni ed attività dislocate nella rete»[37].

La cd. "riservatezza informatica" va, però, distinta dalla "sicurezza informatica", in quanto ha portata più ampia. Infatti, la riservatezza, oltre a proteggere da accessi abusivi nel domicilio informatico, sia ideale che fisico, in cui si trovano i dati informatici relativi alla persona, garantisce anche la «sicurezza e l'esclusività dell'accesso, della gestione e della disponibilità del suo spazio informatico, o meglio cibernetico, vale a dire delle risorse informatiche […] contro ogni interferenza e danneggiamento (essendo l'interesse meritevole di tutela comprensivo della confidenzialità, sicurezza e dunque libertà delle azioni ed elaborazioni, anche solo potenziali o future, realizzabili nel "proprio" ambito esclusivo)»[38]. Dal momento, quindi, che la riservatezza informatica è presupposto dell'esercizio virtuale di altri diritti individuali e collettivi, può essere ricondotta alla categoria degli interessi diffusi, ovvero quegli interessi di cui può usufruire gran parte della popolazione[39].

Concetto per lungo tempo assimilato alla riservatezza è quello di *privacy*. Priva di una definizione riconosciuta a livello internazionale[40], dall'ordinamento italiano è stata sempre

---

[37] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 59-60.

[38] L. PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione,* p. 61-62.

[39] F. MORALES PRATS, *Presupposti politico-criminali per una tutela penale della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo),* in *dir. Inf.*, p. 374. Per "interessi diffusi" si intendono «gli interessi che non fanno capo a un titolare singolo, ad un soggetto determinato, ma riguardano un gruppo o contesto sociale i cui singoli componenti possono usufruire individualmente del bene, senza che la loro identificazione risulti strutturata in un gruppo meglio definito come portatore qualificato e differenziato di un interesse ad esso specifico in quanto dotato di una soggettività. Nel momento in cui tali interessi si strutturano in formazioni sociali più definite, capaci di rappresentanza più associata ed esponenziale, si tende a definirli "collettivi", come tali suscettibili di una tutela processuale più qualificata» M. DONINI, *Teoria del reato: una introduzione,* Padova, 1996, p. 140.

[40] Parte della dottrina statunitense individuava la *privacy* attraverso un elenco "aperto" di tutte le esigenze che riguardavano la sfera privata dell'individuo, tra cui il diritto ad essere lasciati soli, la tutela della propria dignità, personalità e identità, il diritto a tenere determinate questioni segrete agli altri. V. D.J. SOLOVE, *Conceptualizing Privacy,* in *California Law Review,* 2002, p. 1094.

ricondotta al concetto di riservatezza[41]. In passato, in dottrina, si tendeva a definirla come «diritto di mantenere il controllo sulle proprie informazioni»[42].

Ultimamente, però, si tende a far coincidere la *privacy* con il diritto alla protezione dei dati personali, attraverso una concezione "funzionale"[43]. Si ritiene, pertanto, che *privacy* non sia altro che il diritto al corretto trattamento dei dati personali e cioè al loro utilizzo secondo le norme che lo disciplinano. Tale identificazione è stata avvalorata dal fatto che l'insieme delle norme sul trattamento dei dati personali ha preso il nome di "codice della *privacy*".

La maggior parte della dottrina e della giurisprudenza[44], però, si discostano da una simile immedesimazione, poiché ritengono che il diritto alla *privacy* riguardi le informazioni private ed il diritto che queste non subiscano ingerenze, mentre il diritto alla protezione dei dati personali farebbe riferimento ad un concetto più ampio che ricomprende ogni informazione riferibile ad una persona ed il diritto alla tutela di questa, indipendentemente dal fatto che sia privata.

Pertanto, alla luce di tali considerazioni, emerge come i concetti di riservatezza e *privacy* da un lato e quello di protezione dei dati dall'altro, si riferiscano a situazioni giuridiche differenti e non sovrapponibili.

Riservatezza e *privacy*, che nell'ordinamento italiano tendono a coincidere, riguardando la "vita intima" e le "informazioni private", hanno un rilievo spiccatamente individualistico, mentre il corretto trattamento dei dati personali fa riferimento all'interesse, sia individuale che collettivo, alla correttezza e liceità dell'utilizzo dei dati personali.

---

[41] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo regolamento,* Torino, 2016, p. 45.
[42] S. RODOTA', *Repertorio di fine secolo,* 1992, p. 190.
[43] M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *jusonline*, n. 1, 2017, p. 222.
[44] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 45; Corte Giust. UE (Grande Sezione), 6 ottobre 2015, C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, p. 39 e 78.

2. Illecito trattamento dei dati personali e responsabilità degli enti.

Questi nuovi interessi, quindi, sono stati rapidamente messi a rischio dall'evoluzione tecnologica[45], motivo per cui si è reso necessario un intervento europeo sulla regolazione della materia.

Il 24 maggio 2016, infatti, è entrato in vigore il Regolamento n. 679 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati». Tale Regolamento, entrato in vigore il 25 maggio 2018, è stato reso attuativo, in Italia, dal Decreto Legislativo n. 101 del 10 agosto 2018, entrato in vigore il 19 settembre 2018. Quest'ultimo ha provveduto alla novella del cd. Codice della *Privacy* di cui al d. lgs. n.196 del 2003 e successive modificazioni. Il Codice della *Privacy*, pertanto, risulta essere il frutto delle integrazioni apportate dal Regolamento europeo n. 679 del 2016 e del d. lgs. n. 101 del 2018.

In materia di responsabilità degli enti, il d. l. 14 agosto 2013, n. 93, recante «disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province», aveva disposto un integrazione del catalogo[46] dei reati – presupposto del d. lgs. n. 231 del 2001, richiamando, oltre l'art. 640 *ter* c.p. (frode informatica, e l'art. 55 co. 9 del d.lgs. n.231/2007 (utilizzo indebito e falsificazione di carte di credito), anche i delitti contenuti nel Codice della *Privacy* (illecito trattamento di dati personali, falsità nelle dichiarazioni e notificazioni al Garante e inosservanza dei provvedimenti del Garante)[47].

---

[45] Tale concetto viene precisato anche dal Regolamento UE 2016/679, al *considerandum* n. 6, dove si precisa che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali […] la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività […] sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano». Sul punto v. anche M. IASELLI, *Privacy: cosa cambia con il nuovo regolamento europeo,* 2016, p. 1 ss.

[46] Sul punto v. *supra* cap. II, § 2 e 2.1.

[47] Ai sensi dell'art. 9 del d. l. 14 agosto 2013, n. 93, la formulazione dell'art. 24 *bis* del d. lgs. 8 giugno 2001, n. 231, sarebbe stata la seguente: «In relazione alla commissione dei delitti di cui agli articoli 615- ter, 617-quater,

In sede di conversione del decreto, però, è stato eliminato il riferimento ai delitti riguardanti la *privacy* da inserire tra i reati – presupposto della 231. I delitti di cui alla parte III, titolo III, capo II del Codice della *Privacy,* avrebbero potuto apportare un notevole impatto all'interno della *compliance* 231, proprio perché avrebbe interessato l'intera platea delle società commerciali e delle associazioni private soggette alle disposizioni del d.lgs. n. 231/2001. Ma questo avrebbe anche comportato, per le aziende, la necessità di dotarsi di modelli di organizzazione e gestione del trattamento dei dati personali, «nonché, soprattutto in caso di comunicazione di dati personali nell'ambito di gruppi di imprese, specie se a carattere transnazionale, la designazione di un responsabile del trattamento (che nel nuovo regolamento prende il nome di *Data Protection Officer*), che sarebbe diventato un interlocutore privilegiato dell'organismo di vigilanza»[48].

Dopo questo tentativo fallito, nel 2013, l'adeguamento della normativa italiana al Regolamento Europeo n. 679/2016 avrebbe potuto rappresentare una seconda possibilità[49]. Ma l'integrazione dei delitti contro la *privacy*, all'interno del catalogo dei reati – presupposto della responsabilità amministrativa degli enti, non si è concretizzata neanche con il decreto n. 101 del 2018 attuativo del Regolamento.

Pertanto, oggi, il sistema di gestione del trattamento dei dati rimane, nel sistema penale italiano, un fatto circoscritto alla responsabilità delle persone fisiche e non degli enti.

617-quinquies, 635 *bis*, 635 *ter*, 635 *quater*, 635 *quinquies* e 640 *ter*, terzo comma, del codice penale nonché dei delitti di cui agli articoli 55, comma 9, del decreto legislativo 21 novembre 2007, n. 231, e di cui alla parte III, Titolo III, Capo II del decreto legislativo 30 giugno 2003, n. 196, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. (...) 4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel co. 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)»

[48] M. LAMANUZZI, *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, cit., p. 257. V. anche M. ARENA, *I delitti in materia di privacy nel d.lgs. 231/2001,* in *Filodiritto*. Qualora, nell'interesse o a vantaggio dell'ente, soggetti apicali o non apicali, secondo quanto previsto dagli artt. 5 e ss. del d.lgs. 231/2001, avessero commesso delitti in materia di *privacy*, l'ente sarebbe stato assoggettato a una sanzione da 100 a 500 quote (ciascuna delle quali ha un valore che può oscillare da un minimo di 258 a un massimo di 1549 euro).

[49] M. R. PERUGINI – F. RUBINO, *Privacy e tutela penale: evoluzione od occasione o persa?Luci ed ombre della nuova disciplina penale sul trattamento dei dati personali,* in *www.diritto24.ilsole24ore.com,* (3/10/2018).

3. Modelli organizzativi privacy e 231.

Nonostante i vari tentativi di inclusione dei delitti privacy fra i reati presupposto del d.lgs. 231/2001 non siano andati a buon fine, sono, sicuramente, serviti, a mettere in luce degli elementi comuni ai due corpi normativi. Si possono rinvenire, infatti, dei punti di contatto tra il d. lgs. 231/2001 ed il Regolamento Europeo sul trattamento dei dati personali.

È noto che il d. lgs. 231/2001 ha introdotto il concetto di responsabilità amministrativa delle persone giuridiche, secondo il quale nel caso in cui un reato venga commesso dal singolo individuo nell'interesse o a vantaggio dell'ente comporta un coinvolgimento penale dell'azienda stessa.

L'obiettivo finale è sicuramente quello di prevenire la commissione del reato all'interno dell'ente, e questo rischio si può minimizzare attraverso l'adozione di un modello organizzativo adeguato, che, se idoneo, può manlevare la persona giuridica da responsabilità in caso in cui il reato venga commesso.

Così come il d. lgs. 231, anche il Regolamento si focalizza sul concetto di "responsabilizzazione", in quanto punta sull'adozione di comportamenti idonei alla prevenzione dei reati da parte dell'ente e dei soggetti in esso coinvolti.

L'obiettivo di responsabilizzazione è perseguito dal d.lgs. 231 attraverso la previsione di un modello di organizzazione e controllo idoneo a prevenire la commissione dei reati. Per lo stesso obiettivo, il GDPR, fa riferimento al nuovo principio di *accountability*. Con questo termine si fa riferimento all'obbligo di rendicontazione nato in ambito aziendale che serve ad indicare i doveri di trasparenza, «intesa come garanzia della completa accessibilità alle informazioni agli utenti», di responsività, «intesa come la capacità di rendere conto di scelte, comportamenti e azioni» e di *compliance*, «intesa come capacità di far rispettare le norme»[50] .

[50] M. IASELLI, *Privacy: cosa cambia con il nuovo regolamento europeo*, 2016., p. 9. V. anche C. BISTOLFI, *Le obbligazioni di compliance in materia di protezione dei dati*, in L. Bolognini, E. Pelino, C. Bistolfi (a cura

Il GDPR recepisce questo principio all'art. 24, in virtù del quale «tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento», tali «misure sono riesaminate e aggiornate qualora necessario»[51].

Questo modello potrebbe ben definirsi come "modello organizzativo *privacy*", assimilabile, appunto, al modello organizzativo 231.

Altro punto di contatto fra i due corpi normativi è l'approccio comune basato sul rischio. Per poter ottenere il risultato finale di prevenzione della commissione di illeciti (reati o trattamenti inidonei dei dati), occorre analizzare i possibili fattori di rischio. Pertanto, in materia di *privacy,* è necessario individuare una mappatura dei trattamenti, distinti a seconda del grado di rischio, e delle possibili conseguenze per l'interessato. In particolare, per dimostrare di essersi conformato al regolamento, il titolare o il responsabile del trattamento «dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità»[52] nonché «valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi», tenendo in considerazione «i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero

---

di), *Il Regolamento privacy europeo*, *Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, p. 323 e ss.; P. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*: *dalla Direttiva 95/46 al nuovo Regolamento*, Torino, 2016, pp. 282 e ss.

[51] Le eventuali violazioni vanno notificate alle autorità Garanti «*senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*», salvo che «*il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione (accountability), è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche*».

[52] Regolamento UE 2016/679, *considerandum* n. 82. L'art. 30 del regolamento contiene un elenco delle informazioni che devono essere annotate nel registro sulle attività di trattamento. Tuttavia, il *considerandum* n. 13 dispone che, «*per tener conto della specifica situazione delle micro, piccole e medie imprese*», si prevede «*una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni*».

cagionare in particolare un danno fisico, materiale o immateriale»[53] particolare cautela ogniqualvolta il trattamento possa «presentare un rischio elevato per i diritti e le libertà delle persone fisiche»[54].

Inoltre, per poter verificare l'effettivo rispetto delle regole, anche in materia di *privacy*, è necessaria la presenza di un organo di controllo interno. Infatti, così come il d.lgs. 231 prevede la figura dell'Organismo di Vigilanza affinchè il MOG venga effettivamente applicato e rispettato di modo che risulti funzionale alla prevenzione dei reati, il Regolamento Europeo, prevede la figura del *Data Protection Officer*, che è un professionista dotato di competenze informatiche, di analisi, giuridiche e di *risk management*, che ha il compito di organizzare la gestione e il trattamento dei dati personali, nel rispetto delle normative sulla *privacy* nazionali ed europee.

I due "modelli", tuttavia, non sono perfettamente assimilabili.

---

[53] Regolamento UE 2016/679, *considerandum* n. 83. In particolare, il titolare dovrebbe «valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio» (*considerandum* n. 90). «*Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, 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, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti*» (*considerandum* n. 91, in cui si precisa che «*il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati*»).

[54] Regolamento UE 2016/679, *considerandum* n. 84. Inoltre, Il titolare del trattamento ha l'obbligo di dare tempestiva comunicazione delle violazioni sia all'interessato sia alle autorità, v. Regolamento UE 2016/679, art. 34 e *consideranda* n. 86 e 87, in cui si precisa che il titolare debba mettere in atto «*tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali*», n. 88, che prevede l'opportunità di «*definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali*» e n. 89, in cui viene affermata la necessità di superare gli obblighi generali e indiscriminati di notifica previsti dalla direttiva 95/46/CE sostituendoli con «*meccanismi e procedure efficaci che si concentrino su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità*», che «*includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale*».

Innanzitutto, adeguarsi al GDPR è obbligatorio, mentre adottare un modello organizzativo *ex* d.lgs. 231 è facoltativo, è fortemente consigliato ai fini della dimostrazione di innocenza dell'ente a seguito della commissione di un reato al suo interno.

Diversi sono anche i destinatari della formazione. In tema di privacy la formazione è necessaria solo per coloro che sono direttamente sottoposti al trattamento dei dati personali, mentre in ambito 231 i destinatari sono tutti, posto che chiunque può commettere un reato.

Ma la differenza più importante è che il modello 231 prevede una piena esenzione dalla responsabilità nel caso in cui vi sia stata una esatta costruzione, esecuzione ed applicazione del modello organizzativo. Infatti il d. lgs. 231 all'art. 6 con riferimento al reato commesso da chi occupa una posizione apicale all'interno dell'ente, e all'art. 7 con riferimento al reato commesso da soggetto in posizione subordinata, prevede una declaratoria di non responsabilità connessa alla predisposizione di cautele preventive. Nel Regolamento, invece, non è prevista una simile declaratoria. In materia di *privacy* i modelli organizzativi, l'apparato documentale e l'adesione ai codici di condotta categoriali[55] sono elementi che devono essere valutati dall'autorità di controllo e dall'autorità giurisdizionale[56].

[55] Art. 40 Codice Privacy, i codici di condotta sono "regole di condotta" o pratiche uniformi e condivise, elaborate da vari organismi internazionali o anche da singoli Stati, particolarmente diffuse nei rapporti economici internazionali

[56] MESSINA A., *Modelli organizzativi privacy e 231: differenze e possibili sinergie per le imprese*, in *www.ipsoa.it* , 2018.

Conclusioni

Alla luce dell'analisi dei crimini informatici e delle norme che li regolano a livello nazionale e sovranazionale, sono molteplici le conclusioni, e soprattutto le domande, alle quali si giunge.

Innanzitutto va considerata la continua evoluzione sia delle tecnologie informatiche, sia dei reati che approfittano del progresso, sia delle discipline che sono tenute a regolare e ad impedire la crescita di tali abusi. Infatti, con il passare del tempo il progresso tecnologico avanza in maniera esponenziale, e si vanno via via introducendo nuovi strumenti materiali ed immateriali che migliorano la vita dell'individuo e soprattutto entrano a far parte della quotidianità e della vita sociale, culturale, economica e amministrativa dei Paesi. Tuttavia, alla stessa velocità proliferano i crimini perpetrati attraverso i dispositivi informatici e sul Web: crimini nuovi, strettamente legati all'utilizzo dei sistemi, o crimini tradizionali che trovano nelle nuove tecnologie ulteriori prospettive di azione. Le figure dei criminali, allo stesso modo, aumentano continuamente, poiché diventa sempre più semplice acquisire le capacità per commettere reati attraverso i computer e la rete, e al contempo aumentano i metodi per eludere le misure di sicurezza.

Al continuo aggiornamento delle tecnologie e dei crimini ad esse correlati dovrebbe corrispondere un equivalente e costante aggiornamento della produzione normativa che disciplini le fattispecie di reati informatici che vanno configurandosi. Purtroppo, però, questa aspettativa rimane il più delle volte delusa a causa della difficoltà oggettiva di stare al passo con l'implemento costante delle tecnologie.

Il nostro Paese, però, negli ultimi anni, sembra aver acquisito maggior consapevolezza riguardo al problema della minaccia cibernetica. Infatti ha orientato la propria attenzione sul tema della sicurezza attraverso una serie di relazioni presentate dal Governo al Parlamento.

Dunque, molto è stato fatto, molto si sta facendo, ma ancora molto altro è da fare.

Questo perché fin troppo spesso affiorano incertezze interpretative da parte della giurisprudenza in merito alle disposizioni che disciplinano il fenomeno dei crimini informatici, introdotte in Italia dalla l. n. 547/1993 e in alcuni casi modificate dopo la l. n. 48/2008. Infatti dall'analisi emerge una certa disattenzione del legislatore, che potrebbe aver agito in maniera eccessivamente superficiale per rispondere in modo rapido alla necessità di un quadro normativo, trascurando tuttavia aspetti che avrebbero permesso una maggiore chiarezza nell'interpretazione.

Anche a livello sovranazionale tanti passi si stanno compiendo verso una maggiore difesa dello spazio cibernetico, facendo leva soprattutto sulla necessità di cooperazione e coordinazione.

Questo aspetto è essenziale in ragione dei caratteri tipici dei crimini informatici e anche del bisogno di armonizzazione delle norme in una società quanto mai globalizzata.

BIBLIOGRAFIA

AMATO G. - DESTITO V. S. - DEZZANI G. – SANTORIELLO C., *I reati informatici*, 2010.

ARENA M., *I delitti in materia di privacy nel d.lgs. 231/2001,* in *Filodiritto*.

BELLUTA H., *Cybercrime e responsabilità degli enti*, in L. Luparia, *Sistema penale e criminalità informatica*, 2009.

BELLUTA, *Cybercrime e responsabilità degli enti,* in *Sistema penale e criminalità informatica* a cura di LUPARIA, Milano, 2009.

BELTRANI S., *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *La responsabilità amministrativa delle società e degli enti*, n. 4. 2008.

BISTOLFI C., *Le obbligazioni di compliance in materia di protezione dei dati*, in L. Bolognini, E. Pelino, C. Bistolfi (a cura di), *Il Regolamento privacy europeo*, *Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016.

BOEZIO F. - BRUSTIA G., *I crimini informatici*, in S. DI GUARDO - P. MAGGIOLINI - N. PATRIGNANI, *Etica e responsabilità sociale delle tecnologie dell'informazione*, Vol. I, Franco Angeli, 2010.

BRICOLA F., *Prospettive e limiti della tutela penale della riservatezza,* in *Riv. It.dir. proc. Pen.*

CARDUCCI M., *La responsabilità delle persone giuridiche e i crimini informatici*.

Corte Giust. UE (Grande Sezione), 6 ottobre 2015, C-362/14, *Maximilian Schrems c. Data Protection Commissioner*.

CRIMI S., *Commento all'art. 24 bis d.lgs. 231/2001*, pp.306-313, in A. CADOPPI - G. GARUTI -

CUOMO - RAZZANTE*, La nuova disciplina dei reati informatici*, Torino, 2009,

DEZZANI G. - RICCI S., *Reati informatici e responsabilità amministrativa dell'ente*, in G. CASSANO - G. SCORZA - G. VACIAGO, *Diritto dell'internet. Manuale operativo.* Casi, legislazione, giurisprudenza, Cedam, 2012.

DONINI M., *Teoria del reato: una introduzione,* Padova, 1996.

FLOR R., *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in *Dir. Pen. proc.,* 1, 2008.

FLOR R., *Lotta alla "criminalità organizzata" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *dirittopenalecontemporaneo.it*.

FRANCESCHELLI B., *Il diritto alla riservatezza,* Napoli, 1960.

FULVI F. R., *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *dir. Pen. proc*., 2009.

GALDIERI P., in *Interlex*, n. 376, 26 giugno 2008.

IASELLI M, *Privacy: cosa cambia con il nuovo regolamento europeo,* 2016.

LAMANUZZI M., *Diritto penale e trattamento dei dati personali. I reati previsti dal Codice della privacy e la responsabilità amministrativa degli enti alla luce del regolamento 2016/679/UE*, in *jusonline*, n. 1, 2017.

MESSINA A., *Modelli organizzativi privacy e 231: differenze e possibili sinergie per le imprese*, in www.ipsoa.it , 2018.

MODUGNO F., *Ordinamento giuridico*, in *Enc. Dir*., vol. XXX, 1980.

MORALES PRATS F., *Presupposti politico-criminali per una tutela pena della riservatezza informatica (con particolare riguardo all'ordinamento spagnolo),* in *dir. Inf*..

MORGANTE G., sub. art. 7, in *Commento articolo per articolo alla l. 18/3/2008, n. 48*, in *Legisl. pen.*, 2008. .

PARDOLESI R., *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

PECORELLA C., *Il diritto penale dell'informatica*, Padova, rist., 2006, in particolare 306 e ss.

PECORELLA C., *Reati informatici*, in *Enc. Dir.,* 2017.

PERUGINI M. R. – RUBINO F., *Privacy e tutela penale: evoluzione od occasione o persa?Luci ed ombre della nuova disciplina penale sul trattamento dei dati personali,* in www.diritto24.ilsole24ore.com, (3/10/2018).

PESTELLI G., *Brevi note in tema di accesso abusivo ad un sistema informatico o telematico,* in *Cass. pen.,* fasc. 6, 2012.

PICA G., *Diritto penale delle tecnologie informatiche*, Torino, 1999.

PICOTTI L., *Internet e diritto penale: il quadro alla luce dell'armonizzazione internazionale*, in *diritto dell'internet*, 2, 2005.

PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *riv. Trim. dir. Pen. ec*., 4, 2011.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. Pen. proc.,* 2008, 6.

PICOTTI L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. Picotti (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo regolamento,* Torino, 2016.

RESCIGNO P., *Il diritto ad essere lasciati soli,* in *Synteleia per Vincenzo Arangio Ruis,* Napoli, 1964.

RESTA F., *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura*, in *Giurisprudenza di merito*, 2008, 9.

RESTA F., *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica del diritto, giur. Merito*, 11, 2006.

RODOTA' S., *Repertorio di fine secolo,* 1992.

SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica* in L. PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013.

SANTORIELLO C.- DEZZANI G.- DAL CHECCO P., *Delitti informatici e trattamento illecito di dati*, in M. LEVIS - A. PERINI (a cura di), Zanichelli, 2014.

SANTORIELLO C., *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti, in La responsabilità amministrativa delle società e degli enti,* n. 1, 2011.

SOLA, *Prime considerazioni in merito alla legge 547/1993*, in *La nuova normativa in tema di criminalità informatica: alcune riflessioni*, Bologna, 1995

SOLOVE D. J., *Conceptualizing Privacy,* in *California Law Review,* 2002.

SPAGNOLETTI, *Art. 615* ter *c.p.: il domicilio informatico tra profili dogmatici e problemi applicativi*, in *Giur. merito*., 2004.

VACIAGO G., *Internet e i crimini informatici*, in M. L. PICCINI, G. VACIAGO*, Computer crime: casi pratici e metodologie investigative dei reati informatici*, Bergamo, Moretti&Vitali, 2008.

VENEZIANI P., *Enti e responsabilità da reato*, Utet 2010.

WEISMANN M. F., *Internation Cybercrime: Recent Developments in the Law*, in R.D. Clifford (ed.), *Cybercrime*, 2011.

ZENCOVICH Z., *I diritti della personalità dopo la legge sulla tutela dei dati personali,* in *Studium iuris,* 1997.