Dipartimento della Gioventù – POAT Per la Gioventù - CUP J71I09000020007

Supporto allo sviluppo della sicurezza e legalità informatica nell'ambito delle iniziative rivolte ai giovani

Michele Crudele - 2011-07-24

A.1.a) Relazione sulla situazione legislativa riguardante i delitti che coinvolgono i giovani su Internet

Premessa

Poiché lo scopo di questa relazione è la redazione di linee guida per i portali destinati ai giovani, la sua impostazione non è di carattere formale giuridico, ma narrativa con riferimento alle leggi vigenti, riportandone i contenuti più significativi, soprattutto quelli che coinvolgono i giovani. La fonte principale sono i documenti pubblicati dalla Polizia di Stato e da AAMS – Amministrazione Autonoma dei Monopoli di Stato, con semplificazioni, modifiche e adattamenti.

La scelta delle fattispecie delittuose è stata fatta in base alle caratteristiche tipiche dei crimini nei quali sono coinvolti i minori, come protagonisti o vittime, in ordine di gravità e frequenza:

- Pedofilia *online*
- Giochi *online*
- Cyberbullismo
- Frode informatica
- Delitto di accesso abusivo ad un sistema informatico
- Diffusione di computer virus e di apparecchiature dirette a danneggiare o interrompere il funzionamento di un sistema informatico
- Detenzione e la diffusione abusiva di codici di accesso a sistemi informatici
- Danneggiamento di sistemi informatici e telematici
- *Phishing*
- Truffa nel commercio elettronico
- Abuso di carte di credito e debito
- *Spamming*

Oltre alle leggi e agli articoli del codice penale (C.P. o, se evidente, senza citazione) menzionati in questa relazione, nel quadro generale deve essere tenuta presente la Legge 176/91, "Ratifica ed esecuzione della convenzione sui diritti del fanciullo, fatta a New York il 20 novembre 1989".

Mentre la normativa vigente contro gli abusi commessi verso i minori è stringente e severa, includendo fattispecie come la pedopornografia virtuale (utilizzo di immagini artificiali), in altri ambiti si osserva una situazione non sempre coerente per quanto riguarda il bilanciamento tra tutela dei dati personali e accesso alle informazioni per la sicurezza informatica da parte degli amministratori dei sistemi e delle autorità. Il caso del Decreto Pisanu decaduto a fine 2010 dopo diversi anni di proroga è emblematico: la necessità di difesa preventiva dal terrorismo organizzato si scontrava apparentemente con la disponibilità a fornire accesso a reti telematiche, soprattutto senza fili, in modo anonimo. Purtroppo si è confusa la libertà di accesso a Internet con il presunto diritto al completo anonimato e ha vinto l'opinione pubblica favorevole a un accesso senza condizioni, il che comporta una maggiore difficoltà di identificazione di coloro che commettono reati. Uno scenario tipico è l'azione di un malvivente da una rete aperta *wireless* non autenticata, totalmente anonima, che non lascia tracce, collocato in auto davanti a un negozio o una scuola che offrono la navigazione senza fili senza codici di accesso. Siamo in attesa di una normativa che faciliti le operazioni di indagine della Polizia in caso di reati, garantendo la semplicità dell'accesso a Internet.

Pedofilia *online*

Il 2 marzo 2006 è entrata in vigore la Legge n. 38/06 "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet" che introduce delle modifiche alle disposizioni già formulate dalla precedente normativa n. 269/98, così riassunte:

- Riguardo la prostituzione minorile, è punito chi compie atti sessuali con minore di età compresa tra i 14 e i 18 anni, precedentemente l'età era compresa tra i 14 e i 16 anni.
- Il reato di pornografia minorile si delinea quando utilizzando minori degli anni 18 di realizzano esibizioni pornografiche o si produce materiale pornografico o si induce i minori di anni 18 a partecipare a dette esibizioni.
- Per buona parte dei delitti in materia di sfruttamento sessuale dei minori si esclude la possibilità di ricorrere al patteggiamento "allargato".
- Nel caso di condanna si applica sempre come pena accessoria l'interdizione perpetua da qualunque incarico nelle scuole o strutture pubbliche o private che siano frequentate prevalentemente da minori.
- Gli operatori turistici sono obbligati ad inserire nei materiali propagandistici la comunicazione sulla punibilità dei reati di pornografia e prostituzione minorile anche se commessi all'estero.
- Viene creato un nuovo organismo per il contrasto della lotta contro la pedopornografia sulla rete Internet il "Centro Nazionale di monitoraggio della pornografia minorile sulla Rete", con il compito di raccogliere segnalazioni sull'andamento del fenomeno.
- Responsabilità e obblighi per i fornitori di servizi (provider).
- Collaborazione con gli Istituti di credito, Poste Italiane e intermediari finanziari nell'ambito di indagini che vedono coinvolti soggetti che eseguono transizioni finanziarie in rete per l'acquisto e/o la vendita di materiale pedopornografico.
- Per la prima volta viene perseguita anche la fattispecie riguardante "immagini realizzate con tecniche di elaborazioni grafiche" aventi ad oggetto minori per i quali, inoltre, è esteso l'arresto obbligatorio in flagranza.

La Legge n. 269 del 3 agosto 1998, titolata "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù", aveva introdotto nel codice penale ed in quello di procedura penale importanti novità atte a permettere, alle Forze di Polizia ed alla Magistratura, un contrasto maggiormente incisivo del fenomeno dello sfruttamento sessuale dei minori, con particolare riguardo alla cosiddetta pedofilia *online*.

La Legge in argomento così come integrata dalla suindicata Legge n. 38/06 ha introdotto nel codice penale alcuni articoli che disciplinano nuove figure di reato.

Induzione, favoreggiamento e sfruttamento della prostituzione di minori.

L'articolo 600 bis del codice penale, titolato "Prostituzione minorile" recita:

> Chiunque induce alla prostituzione una persona di età inferiore agli anni diciotto ovvero ne favorisce o sfrutta la prostituzione è punito con la reclusione da sei a dodici anni e con la multa da euro 15.493 a euro 154.937.
>
> Salvo che il fatto costituisca più grave reato, chiunque compie atti sessuali con un minore di età compresa tra i quattordici e diciotto anni, in cambio di denaro o di altra utilità economica, è punito con la reclusione da sei mesi a tre anni e con la multa non inferiore a euro 5.164.
>
> Nel caso in cui il fatto di cui al secondo comma sia commesso nei confronti di persona che non abbia compiuto gli anni sedici, si applica la pena della reclusione da due a cinque anni.

> Se l'autore del fatto di cui al secondo comma è persona minore di anni diciotto si applica la pena della reclusione o della multa, ridotta da un terzo a due terzi.

Produzione, commercio, distribuzione, divulgazione e cessione di materiale pornografico coinvolgente minori.

L'articolo 600 ter intitolato "Pornografia minorile" dispone che:

> Chiunque, utilizzando minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche è punito con la reclusione da sei a dodici anni e con la multa da euro 25.822 a euro 258.228.
>
> Alla stessa pena soggiace chi fa commercio del materiale pornografico di cui al primo comma.
>
> Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro 51.645.
>
> Chiunque, al di fuori delle ipotesi di cui ai commi primo, secondo e terzo, offre o cede ad altri anche a titolo gratuito, il materiale pornografico di cui al primo comma, è punito con la reclusione fino a tre anni e con la multa da euro 1.549 a euro 5.164.
>
> Nei casi previsti dal terzo e dal quarto comma la pena è aumentata in misura non eccedente i due terzi ove il materiale sia di ingente quantità.

Detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori.

L'articolo 600 quater, titolato "Detenzione di materiale pornografico", recita:

> Chiunque, al di fuori delle ipotesi previste dall'art.600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549.
>
> La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità.

La stessa Legge inserisce dopo il 600 quater il 600 quater.1 che introduce la Pornografia Virtuale e detta:

> Le disposizioni di cui agli articoli 600 ter e 600 quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo.
>
> Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Pene accessorie

> La condanna o l'applicazione della pena su richiesta delle parti a norma dell'art.444 del codice di procedura penale per uno dei delitti di cui al primo comma comporta in ogni caso l'interdizione perpetua da qualunque incarico nelle scuole di ogni ordine e grado, nonché da ogni ufficio o servizio in istituzioni o strutture pubbliche o private frequentate prevalentemente da minori.

Ulteriore novità introdotte dalla Legge 269/98 e successive modificazioni, sono rappresentate anche dall'attribuzione di poteri investigativi al Servizio della Polizia Postale e delle Comunicazioni,

indicato quale Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

Nell'ambito del contrasto alla diffusione di immagini pedoponografiche su Internet, l'articolo 14 (comma 1 e 2) della Legge in argomento consente alla Polizia Postale e delle Comunicazioni (a seguito di precisa autorizzazione dell'Autorità Giudiziaria):

- Di procedere ad acquisti simulati ed a scambio di materiale pedopornografico
- Di attivare siti web sotto copertura
- Di "navigare" nella rete Internet con agenti sotto copertura
- Di partecipare, con i propri agenti (infiltrati), ad iniziative di turismo sessuale.

La Legge 38/2006 ha rinforzato, ulteriormente, l'apparato normativo di contrasto alla pedopornografia sulla rete, introducendo l'art. 14 bis che così detta:

> Presso l'organo del Ministero dell'Interno di cui al comma 2 dell'articolo 14, è istituito il Centro Nazionale per il contrasto della pedopornografia sulla rete Internet, di seguito denominato "Centro", con il compito di raccogliere tutte le segnalazioni, provenienti anche dagli organi di polizia stranieri e da soggetti pubblici e privati impegnati nella lotta alla pornografia minorile, riguardanti siti che diffondono materiale concernente l'utilizzo sessuale dei minori avvalendosi delle rete Internet e di altre reti di comunicazione, nonché i gestori e gli eventuali beneficiari dei relativi pagamenti. Alle predette segnalazioni sono tenuti gli agenti e gli ufficiali di polizia giudiziaria. Ferme restando le iniziative e le determinazioni dell'autorità giudiziaria, in caso di riscontro positivo il sito segnalato, nonché i nominativi dei gestori e dei beneficiari dei relativi pagamenti, sono inseriti in un elenco costantemente aggiornato.

Sono altresì previsti obblighi dei fornitori di servizi che in base al nuovo articolo 14 ter e 14 quater sono obbligati a:

- Fermo restando quanto previsto da altre leggi o regolamenti a segnalare al Centro le imprese e i soggetti che, a qualsiasi titolo diffondono, distribuiscono o fanno commercio, anche in via telematica, di materiale pedoponografico.
- Su richiesta del Centro gli stessi devono comunicare ogni informazione relativa a contratti con tali imprese e soggetti.
- I fornitori dei servizi devono conservare il materiale oggetto della segnalazione per almeno quarantacinque giorni.
- I fornitori di connettività, al fine di impedire ai siti segnalati dal Centro, sono obbligati ad utilizzare strumenti di filtraggio e soluzioni tecnologiche conformi ai requisiti individuati con decreto del Ministro delle comunicazioni di concerto con il Ministro per l'innovazione e le tecnologie e sentite le associazioni maggiormente rappresentative dei fornitori di connettività.

Giochi *online*

I principali riferimenti normativi che disciplinano l'azione di contrasto al fenomeno del gioco illegale online sono la Legge 27 dicembre 2006, n. 296, art. 1 comma 50, "Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato" (legge finanziaria 2007, che ha abrogato e sostituito l'art. 1, commi 535 - 538, della Legge 23 dicembre 2005, n. 266) e il Decreto Direttoriale AAMS n. 1034/CGV del 2 gennaio 2007, attuativo della suindicata normativa e concernente "la rimozione dei casi di offerta, attraverso rete telematica, di giochi, lotterie, scommesse o concorsi pronostici con vincite in denaro in assenza di concessione, autorizzazione, licenza od altro titolo autorizzatorio o abilitativo o, comunque, in violazione delle norme di legge o di regolamento o dei limiti o delle prescrizioni definite da AAMS". Con questo decreto di "inibizione dei siti di gioco non autorizzati", si dà attuazione alle disposizioni contenute nell'articolo 1 della Legge Finanziaria 2006, con lo scopo di contrastare le truffe *online* connesse al gioco d'azzardo.

A completamento, infine, del quadro normativo va segnalato il Decreto Direttoriale AAMS n. 1484 del 10 giugno 2008, che definisce le modalità di applicazione delle sanzioni amministrative pecuniarie da irrogare, ai sensi della Legge 24 novembre 1981, n. 689, nei confronti dei fornitori dei servizi di rete, in caso di mancata inibizione dei siti di gioco non autorizzati.

Nella Legge 7 luglio 2009, n. 88 sulle Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee, sono adottati accorgimenti ulteriori "al fine di contrastare in Italia la diffusione del gioco irregolare ed illegale, nonché di perseguire la tutela dei consumatori e dell'ordine pubblico, la tutela dei minori e la lotta al gioco minorile ed alle infiltrazioni della criminalità organizzata nel settore dei giochi, tenuto conto del monopolio statale in materia di giochi" e in particolare si impone la "adozione ovvero messa a disposizione di strumenti ed accorgimenti per l'autolimitazione ovvero per l'autoesclusione dal gioco, l'esclusione dall'accesso al gioco da parte di minori, nonché l'esposizione del relativo divieto in modo visibile negli ambienti virtuali di gioco gestiti dal concessionario".

Nella Legge di stabilità 2011 (Legge 13 dicembre 2010, n. 220 pubblicata sulla G.U. n.297 del 21/12/2010) è stato introdotto un principio che si applica a ogni tipo di gioco pubblico, ampliando quindi il divieto che prima era limitato a specifiche apparecchiature di gioco come riportato nell'art. 110 del testo unico delle leggi di pubblica sicurezza (TULPS).

L'Art. 24 comma 20 della Legge di stabilità recita:

> È vietato consentire la partecipazione ai giochi pubblici con vincita in denaro ai minori di anni diciotto.

Art. 24 comma 21.

> Il titolare dell'esercizio commerciale, del locale o, comunque, del punto di offerta del gioco che consente la partecipazione ai giochi pubblici a minori di anni diciotto è punito con la sanzione amministrativa pecuniaria da euro cinque mila a euro venti mila. Indipendentemente dalla sanzione amministrativa pecuniaria e anche nel caso di pagamento in misura ridotta della stessa, la violazione prevista dal presente comma è punita con la chiusura dell'esercizio commerciale, del locale o, comunque, del punto di offerta del gioco da dieci fino a trenta giorni; ai fini di cui al presente comma, il titolare dell'esercizio commerciale, del locale o, comunque, del punto di offerta del gioco, all'interno dei predetti esercizi, identifica i giocatori mediante richiesta di esibizione di un idoneo documento di riconoscimento. Le sanzioni amministrative previste nei periodi precedenti sono applicate dall'ufficio territoriale dell'Amministrazione autonoma dei monopoli di Stato competente in relazione al luogo e in ragione dell'accertamento eseguito. Per le cause di opposizione ai

> provvedimenti emessi dall'ufficio territoriale dell'Amministrazione autonoma dei monopoli di Stato è competente il giudice del luogo in cui ha sede l'ufficio che ha emesso i provvedimenti stessi. Per i soggetti che nel corso di un triennio commettono tre violazioni, anche non continuative, del presente comma è disposta la revoca di qualunque autorizzazione o concessione amministrativa; a tal fine, l'ufficio territoriale dell'Amministrazione autonoma dei monopoli di Stato che ha accertato la violazione effettua apposita comunicazione alle competenti autorità che hanno rilasciato le autorizzazioni o concessioni ai fini dell'applicazione della predetta sanzione accessoria.

Nel mese di giugno 2011 i conti di gioco attivi in Italia sono stati 978.048. La diminuzione rispetto al passato è in parte dovuta all'avvio, a giugno, di controlli più stringenti sui dati dichiarati dai giocatori da parte dei concessionari, grazie ai nuovi strumenti messi loro a disposizione da AAMS (verifica del codice fiscale tramite l'anagrafe tributaria), in previsione del passaggio al nuovo regime introdotto dalla Legge 88 del 2009 (poi avvenuto formalmente il 7 luglio 2011). Questa operazione ha certamente consentito di ridurre il numero di minori che giocavano utilizzando falsi codici fiscali.

Cyberbullismo

Gli atti di bullismo attraverso mezzi telematici non costituiscono una fattispecie penale a sé. Possono essere inquadrati negli "atti persecutori" di cui all'articolo 612 bis del Codice penale, in analogia con lo *stalking*:

> Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.
>
> La pena è aumentata se il fatto è commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa.
>
> La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata.
>
> Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.

Il cyberbullismo può includere o provocare successivamente altri reati, come

- Percosse (art. 581 C.P.)
- Lesioni personali (art. 582 C.P.)
- Violenza privata (art. 610 C.P.)
- Lesione personale gravissima (art. 583,2 C.P.)
- Ingiuria (art. 594 C.P.)
- Diffamazione (art. 595 C.P.)
- Minaccia (art. 612 C.P.)
- Molestia (art. 660 C.P.)
- Violenza sessuale (art. 609 bis C.P.)
- Danneggiamento (art. 635 C.P.)
- Furto (art. 624 C.P)
- Estorsione (art. 629 C.P.)
- Violazione della privacy (D. lgs. 196/2003)

Un ulteriore elenco di violazioni è elencato al punto 2 della direttiva 104/2007 del Ministero della Pubblica Istruzione emessa in conseguenza dell'aumento dei casi di bullismo nelle scuole dopo l'episodio di fine 2006 conosciuto per la pubblicazione su YouTube di un filmato di vessazioni di un disabile mentale dell'Istituto Steiner di Torino. Il Ministro istituì una commissione speciale "Bullismo a scuola" di cui l'autore di questa relazione ha fatto parte come esperto informatico.

È utile riportare il testo completo della direttiva che è tuttora vigente perché costituisce un'ampia esposizione del problema con la descrizione delle conseguenze disciplinari e legali.

Ministero della Pubblica Istruzione direttiva 104 del 30 novembre 2007

> CONSIDERATO che il diritto alla protezione dei dati personali gode di specifiche forme di tutela stante la vigenza di apposite disposizioni normative (da ultimo, contenute nel "Codice in materia di protezione dei dati personali", approvato con d.lgs. 30 giugno 2003 n. 196) volte ad assicurare che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle

libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza e all'identità personale;

CONSIDERATO che il Ministero della pubblica istruzione intende promuovere fra gli studenti la più ampia conoscenza dei diritti di rilevanza costituzionale, quale è il diritto alla protezione dei dati personali, nella convinzione che l'educazione alla cultura della legalità deve essere effettuata mediante azioni volte a favorire la conoscenza ed il rispetto delle leggi vigenti;

CONSIDERATO che per gli studenti il diritto alla riservatezza è sancito espressamente anche dall'art. 2, comma 2, del d.P.R. 24 giugno 1998 n. 249 (c.d. "Statuto delle studentesse e degli studenti"), richiamato dall'art. 96, comma 2, del predetto Codice;

CONSIDERATO che nell'ambito delle comunità scolastiche, soprattutto tra i giovani, risulta molto frequente l'utilizzo di "telefoni cellulari" o di altri dispositivi elettronici;

CONSIDERATO che la regolamentazione delle sanzioni disciplinari applicabili nei confronti degli studenti per la violazione del divieto di utilizzo dei telefoni cellulari o di altri dispositivi elettronici durante lo svolgimento di attività didattiche è rimessa all'autonomo potere organizzativo-regolamentare delle istituzioni scolastiche conformemente a quanto chiarito con l'atto di indirizzo del Ministro della Pubblica Istruzione prot. n. 30/DIP/segr. del 15 marzo 2007 avente ad oggetto "linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";

che la regolamentazione dell'utilizzo delle suddette apparecchiature da parte del personale docente è disciplinata, oltre che da disposizioni organizzative previste dall'autonoma regolamentazione di istituto, da specifiche norme deontologiche e disciplinari, dettate dallo Statuto dei lavoratori e dal CCNL in coerenza con l'esigenza di adempiere correttamente ai doveri professionali;

che, indipendentemente dai summenzionati profili organizzativi-sanzionatori inerenti all'ordinamento scolastico e connessi ad un utilizzo improprio dei telefoni cellulari o di altri dispositivi elettronici volto a turbare il corretto e sereno svolgimento delle attività didattiche, si pone il problema di chiarire se in via più generale, ai sensi dell'ordinamento vigente, siano configurabili fattispecie in contrasto con la normativa sulla protezione dei dati personali;

che nelle istituzioni scolastiche ha assunto vasta diffusione e rilevanza sociale il fenomeno dell'utilizzo di telefoni cellulari o di altri dispositivi elettronici, da parte degli studenti o di altri soggetti, allo scopo di acquisire, rectius "carpire", dati in formato audio, video o immagine che riproducono registrazioni vocali o filmati o fotografie digitali riconducibili a persone, studenti, docenti, o altri soggetti, che operano all'interno della comunità scolastica;

CONSIDERATO che i dati in questione si configurano come "dati personali" ai sensi dell'art. 4, comma 1, lettera b) del predetto Codice;

CONSIDERATO che l'acquisizione dei dati sopra menzionati, pur svolgendosi all'interno delle istituzioni scolastiche, in molti casi, non è riconducibile allo svolgimento di attività didattiche, formative o di apprendimento proprie della scuola;

CONSIDERATO che i dati di cui sopra vengono frequentemente divulgati non solo tra gli appartenenti alla stessa comunità scolastica ma, talvolta, anche verso un pubblico "indistinto" di fruitori mediante l'utilizzo dei sistemi telematici e della rete internet;

CONSIDERATO che si assiste alla crescente diffusione nella rete internet di siti web e portali "dedicati" volti a rendere pubblici filmati o registrazioni aventi per oggetto episodi verificatisi nell'ambito delle istituzioni scolastiche o comunque durante i periodi di

svolgimento di attività didattiche o formative, in alcuni casi, anche con finalità denigratorie della dignità personale e sociale di studenti, anche minori di età, e docenti;

CONSIDERATO che i dati personali sopra menzionati sono in alcuni casi "sensibili";

CONSIDERATO che, alla luce di quanto sopra illustrato, si rendono necessari ulteriori chiarimenti interpretativi, oltre a quelli già forniti con il provvedimento a carattere generale del Garante per la protezione dei dati personali del 20 gennaio 2005 e con il precedente provvedimento del 12 marzo 2003, con particolare riferimento alle fattispecie concrete che vengono a configurarsi nelle scuole italiane;

CONSIDERATA l'esigenza di fornire opportuni chiarimenti esplicativi della normativa vigente al fine di favorire il pieno rispetto della disciplina di protezione dei dati e di informare i soggetti della comunità scolastica circa le conseguenze sanzionatorie che possono prodursi nei confronti di chi incorre nella violazione del diritto alla protezione dei dati personali;

CONSIDERATA l'opportunità di porre in essere attività informative nelle scuole allo scopo di prevenire il fenomeno della violazione del diritto fondamentale alla protezione dei dati personali, di derivazione costituzionale, da parte degli studenti e degli altri soggetti della comunità scolastica;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);

VISTO il Decreto del Ministro della Pubblica Istruzione 7 dicembre 2006, n. 305 "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli artt. 20 e 21 del D.Lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (pubblicato sulla G.U. n. 11 del 15 gennaio 2007);

VISTA la legge 15 marzo 1999 n. 59;

VISTO il DPR 8 marzo 1999 n. 275;

VISTO il DPR 24 giugno 1998 n. 249, "Statuto delle studentesse e degli studenti";

VISTA la Direttiva del Ministro della Pubblica Istruzione prot. n. 5843/A3 del 16 ottobre 2006, recante: "Linee di indirizzo sulla cittadinanza democratica e legalità";

VISTA la Direttiva del Ministro della Pubblica Istruzione, prot. n. 1455 del 10 novembre 2006, recante " Indicazioni ed orientamenti sulla partecipazione studentesca"

VISTA la Direttiva del Ministro della Pubblica Istruzione, prot. n. 16 del 5 febbraio 2007, recante "linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo";

VISTO l'atto di indirizzo del Ministro della Pubblica Istruzione, prot. n. 30/dip./segr. del 15 marzo 2007, recante "linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione

di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti";

VISTO l'art. 4 comma 1 lettera A, D.L.vo 30 marzo 2001, n. 165;

SENTITO il parere del Garante per la protezione dei dati personali nella seduta del 29 novembre 2007, ai sensi dell'art. 154, comma 4, del predetto Codice ;

ADOTTA

la presente direttiva recante linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali.

1. Uso dei telefoni cellulari allo scopo di acquisire dati personali

Le immagini, i suoni e i filmati acquisiti nelle comunità scolastiche mediante telefoni cellulari o altri dispositivi elettronici e successivamente trasmessi tramite MMS o comunque divulgati in altre forme, ivi compresa la pubblicazione su siti Internet, possono contenere informazioni di carattere personale relative ad uno o più interessati identificati o identificabili e in particolare a persone fisiche. Ne segue che la raccolta, conservazione, utilizzazione e divulgazione a terzi dei predetti dati configura, ai sensi della normativa vigente, un "trattamento" di dati personali.

Tali dati, peraltro, possono anche riguardare la sfera della salute, della vita sessuale o altre informazioni "sensibili" per cui sono previste particolari garanzie a tutela degli interessati.

Sembra opportuno ricordare che per "dati sensibili" si intendono: "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (cfr. art. 4 comma 1 lettera C del Codice della privacy).

La disciplina in materia di protezione dei dati personali, invece, non si applica quando i dati raccolti non comprendono informazioni riferite a soggetti identificati o identificabili, anche indirettamente.

Ciò posto, corre l'obbligo di chiarire gli ambiti di operatività della normativa vigente mettendo in evidenza che si devono distinguere due diverse situazioni giuridiche a seconda che l'acquisizione dei dati personali in questione sia finalizzata ad una successiva divulgazione verso terzi oppure avvenga esclusivamente per un uso personale.

2. Specifiche cautele di carattere generale

Chi utilizza ed invia i dati personali raccolti (immagini, filmati, registrazioni vocali,…), indipendentemente dal fatto che lo faccia per fini personali o per diffonderli, anche successivamente, deve rispettare in ogni caso gli specifici obblighi previsti a tutela dei terzi dalla comune disciplina in campo civile e penale, anche nel caso di uso dei dati per fini esclusivamente personali.

La raccolta, la comunicazione e l'eventuale diffusione di immagini e suoni deve avere comunque luogo nel rispetto dei diritti e delle libertà fondamentali degli interessati, utilizzando l'immagine altrui nei modi e nei casi consentiti dall'ordinamento.

Si dovrà quindi porre attenzione, in particolare, sulla tutela prevista dall'art. 10 del codice civile ("Abuso dell'immagine altrui").

"Articolo 10 Abuso dell'immagine altrui

Qualora l'immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l'esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l'autorità giudiziaria, su richiesta dell'interessato, può disporre che cessi l'abuso, salvo il risarcimento dei danni".

Pari attenzione deve essere prestata alle garanzie previste per l'esposizione, la riproduzione e la messa in commercio non consensuali del ritratto di una persona (art. 96 legge 22 aprile 1941, n. 633 sul diritto d'autore), le quali richiedono il consenso della persona ritrattata a meno che la riproduzione dell'immagine sia giustificata "dalla notorietà o dall'ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico" e vietano, comunque, l'esposizione o la messa in commercio

che rechino "pregiudizio all'onore, alla reputazione od anche al decoro della persona ritrattata" (art. 97, comma 1, della legge 22 aprile 1941 n. 633).

Inoltre, il dovere di astenersi dal violare queste prerogative degli interessati anche in applicazione del principio del "neminem laedere" (art. 2043 codice civile) non esaurisce gli obblighi giuridici della persona che utilizza i suddetti dati personali (immagini, filmati, registrazioni vocali,…), dovendo la stessa rispettare altri divieti sanzionati penalmente che possono riguardare, in particolare:

a) l'indebita raccolta, la rivelazione e la diffusione di immagini attinenti alla vita privata che si svolgono in abitazioni altrui o in altri luoghi di privata dimora (art. 615-bis codice penale);

b) il possibile reato di ingiurie, in caso di particolari messaggi inviati per offendere l'onore o il decoro del destinatario (art. 594 codice penale);

c) le pubblicazioni oscene (art. 528 codice penale);

d) la tutela dei minori riguardo al materiale pornografico (artt. 600-ter codice penale; legge 3 agosto 1998, n. 269).

Di conseguenza, chi utilizza dati personali (immagini, filmati, registrazioni vocali,…), raccolti con il proprio cellulare o altri dispositivi, deve vagliare tutte queste circostanze e porre attenzione a che i propri comportamenti non ledano i diritti dei terzi, ad esempio evitando di riprendere persone in atteggiamenti o situazioni che possano lederne la dignità o astenendosi dal divulgare immagini, anche occasionalmente, ad un numero elevato di soggetti senza che la persona fotografata o filmata ne sia a conoscenza e possa attivarsi al fine di tutelare la propria sfera privata.

3. Divulgazione dei dati

Come è noto, i moderni telefoni cellulari, così come altri dispositivi elettronici, consentono facilmente, ed in ogni momento, agli utenti di scattare fotografie o registrare suoni o filmati, riconducibili a delle persone fisiche. Tali strumenti consentono anche l'invio ad altre persone delle fotografie o delle registrazioni sopra citate, ad esempio mediante l'utilizzo di "MMS", oltre ad offrire la possibilità di utilizzare i suddetti dati per la pubblicazione su siti internet.

Di fronte a queste opportunità fornite dall'utilizzo delle nuove tecnologie occorre chiarire che la diffusione di dati personali di questo genere, ai sensi della normativa vigente, non può avvenire sulla base della libera volontà di chi li ha acquisiti, in quanto ciascuna persona è titolare del diritto alla protezione dei dati personali. Di conseguenza, la diffusione o la comunicazione in via sistematica di dati personali, quali quelli anzidetti, specie se ad una pluralità di destinatari, può avvenire soltanto dopo che la persona interessata sia stata debitamente informata in ordine alle successive modalità di utilizzo dei dati, con particolare riferimento all'eventualità che i dati siano diffusi o comunicati sistematicamente, ed abbia manifestato il suo consenso (ai sensi degli artt. 13 e 23 del predetto Codice). Nel caso di dati sensibili il consenso dovrà essere espresso in forma scritta, fermo restando comunque il divieto di divulgare dati sulla salute.

Tali regole di carattere generale valgono anche nell'ambito delle comunità scolastiche nelle quali assume un particolare significato culturale nei confronti dei giovani l'esigenza di assicurare la conoscenza ed il rispetto delle norme poste a tutela dei diritti dei singoli. Ciò significa che gli studenti, i docenti o altri soggetti della comunità scolastica che vorranno scattare delle fotografie o effettuare registrazioni audio o video all'interno delle istituzioni scolastiche, con il proprio telefono cellulare o altri dispositivi, e successivamente utilizzare, divulgare, inviare i dati personali acquisiti sono obbligati a porre in essere due adempimenti:

A – si deve informare la persona interessata circa:

le finalità e le modalità del trattamento che si intende effettuare in relazione a tali dati;

i diritti di cui è titolare in base all'art. 7 del Codice , quali, ad esempio, il diritto di ottenere la cancellazione o la trasformazione in forma anonima dei dati personali;

gli estremi identificativi di colui che usa il telefono cellulare o altri dispositivi per raccogliere i dati.

B – deve acquisire il consenso espresso dell'interessato. Nel caso in cui il trattamento riguardi dati di tipo sensibile, occorre acquisire il consenso in forma scritta, fermo restando il predetto divieto di divulgare i dati sulla salute.

L'inosservanza dell'obbligo di preventiva informativa all'interessato comporta il pagamento di una sanzione amministrativa che va da un importo minimo di 3.000 euro sino ad un massimo di 18.000 euro ovvero, in caso di dati sensibili o di trattamenti che comportino situazioni di pregiudizio, di grave detrimento anche con eventuale danno, la sanzione va da un minimo di 5.000 euro sino ad un massimo di 30.000 euro (cfr. art. 161 del Codice).

3.1 Uso personale

Nell'ipotesi in cui, viceversa, i filmati, le immagini o i suoni, relativi ad altre persone, siano acquisiti mediante telefonino per "fini esclusivamente personali" non operano i predetti obblighi di informativa e di acquisizione del consenso in materia di trattamento dei dati personali. Ciò, tuttavia, a condizione che le informazioni così raccolte "non siano destinate ad una comunicazione sistematica o alla diffusione".

Gli obblighi di informativa e di acquisizione del consenso non operano ad esempio, come chiarito dal Garante per la protezione dei dati personali, nel caso dello scatto di una fotografia e del suo invio occasionale (ad esempio, ad amici o familiari): il soggetto che la scatta o che effettua la ripresa con il proprio telefono mobile soddisfa esclusivamente esigenze di carattere strettamente personale (culturali, di svago o di altro genere) e le immagini comunicate restano in un ambito circoscritto di conoscibilità.

Gli obblighi in questione risultano, al contrario, applicabili nel diverso caso in cui, benché per scopi anche semplicemente culturali o informativi, l'immagine sia raccolta per essere diffusa in Internet o comunicata sistematicamente a terzi.

Tra queste due ipotesi, come è stato spiegato sempre dal Garante, vi possono essere peraltro situazioni-limite alle quali va posta particolare attenzione e che vanno esaminate caso per caso.

A titolo esemplificativo si fa presente che i dati personali in questione (immagini, filmati, registrazioni vocali,…) possono essere inviati, ad esempio tramite MMS, con una sola comunicazione a terzi diretta, però, ad un numero assai ampio di destinatari. Qui si possono determinare condizioni pratiche nelle quali l'invio pur occasionale dell'immagine avviene con caratteristiche tali da dar vita ad una comunicazione a catena di dati.

In ogni caso, resta fermo che anche l'utilizzo di immagini, filmati o registrazioni vocali per fini esclusivamente personali deve rispettare comunque l'obbligo di mantenere sicure le informazioni raccolte, tenendo conto che il rispetto dei diritti, delle libertà fondamentali e della dignità dei terzi interessati è sotteso anche a questi trattamenti e che se si cagiona a terzi un eventuale danno anche non patrimoniale colui che utilizza in modo improprio le immagini o altri dati personali, raccolti con il cellulare o con analogo dispositivo elettronico, deve risarcirlo se non prova di aver adottato tutte le misure idonee ad evitarlo.

4. Regolamenti di istituto e sanzioni disciplinari

Gli studenti che non rispettano gli obblighi sopra richiamati, di preventiva informativa, nei casi che lo prevedono, commettono una violazione, punita con una sanzione amministrativa, della cui applicazione è competente il Garante (artt. 161 e 166 del Codice).

In ogni caso, gli studenti devono adottare un comportamento corretto e di rispetto nei confronti del dirigente scolastico, del personale della scuola e dei loro compagni, con riferimento al quale i regolamenti delle singole istituzioni scolastiche individuano i comportamenti che configurano mancanze disciplinari (artt. 3 e 4, d.P.R. 24 giugno 1998, n. 249 – "Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria").

Ne segue che tali comportamenti, connessi ad un trattamento improprio di dati personali acquisiti mediante telefoni cellulari o altri dispositivi elettronici, devono essere sanzionati con opportuno rigore e severità nell'ambito dei regolamenti delle singole istituzioni scolastiche. Le scuole sono dunque tenute a conformare i propri regolamenti secondo i chiarimenti sopra illustrati individuando, nell'ambito della propria autonomia, le sanzioni più appropriate da irrogare nei confronti degli studenti che violano il diritto alla protezione dei dati personali all'interno delle comunità scolastiche.

Si deve infine richiamare l'attenzione sulla possibilità da parte delle istituzioni scolastiche autonome, nei propri regolamenti, di inibire, in tutto o in parte, o di sottoporre opportunamente a determinate cautele, l'utilizzo di videotelefoni e di MMS all'interno delle scuole stesse e nelle aule di lezione.

L'istituzione scolastica è infatti dotata del potere di dettare delle apposite disposizioni organizzative interne all'istituto volte a disciplinare l'utilizzo dei c.d. MMS da parte degli studenti, ad esempio vietando l'utilizzo delle fotocamere, delle videocamere o dei registratori vocali, inseriti all'interno di telefoni cellulari o di altri dispositivi elettronici, in assenza di un esplicito consenso manifestato dall'interessato.

La violazione di tali regole contenute nei regolamenti di istituto può dunque configurare un'infrazione disciplinare, con conseguente applicazione della relativa sanzione individuabile dalla scuola stessa.

In considerazione della vasta rilevanza sociale che ha assunto il fenomeno dell'utilizzo dei telefoni cellulari per l'acquisizione ed il trattamento di dati personali nell'ambito delle scuole italiane, risulta particolarmente auspicabile l'adozione delle misure sopra indicate unitamente all'individuazione di spazi di riflessione e di studio in ordine alle problematiche oggetto della presente direttiva al fine di favorire tra i giovani la consapevolezza dell'importanza del diritto alla protezione dei dati personali nell'ordinamento vigente nell'ottica di diffondere la cultura della legalità.

Il Ministero della Pubblica Istruzione, in collaborazione con il Garante per la Protezione dei Dati Personali, promuoverà iniziative di informazione e formazione rivolte ai dirigenti scolastici al fine di diffondere nelle scuole la più ampia conoscenza della normativa inerente l'esercizio del diritto alla protezione dei dati personali e le relative tutele.

IL MINISTRO

Giuseppe Fioroni

Frode informatica

L'articolo 10 della legge 547/93, anche detta legge sui "*computer crime*", ha inserito nel codice penale l'articolo 640 ter intitolato "Frode informatica". Questo articolo è stato inserito nel capo II del codice penale che è dedicato ai "Delitti contro il patrimonio mediante frode":

> 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 essi 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 51 a 1032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 a 1549 euro se ricorre una delle circostanze previste dal secondo comma numero 1 dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore di sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

Il tipico modo di operare è quello di alterare o immettere abusivamente dati all'interno di un computer oppure quello di modificare un programma così che, una volta in esecuzione, possa far ottenere profitto illegale al colpevole. Un modo di operare, spesso utilizzato, è alterare il *software* installato all'interno delle macchinette di video poker, così da rendere molto bassa la possibilità di vincita del giocatore. Questa condotta può essere facilmente ricompresa nel dettato dell'articolo poiché vi è l'intervento senza diritto su un programma contenuto in un sistema informatico con finalità, da parte del gestore, di conseguire un ingiusto profitto tale da arrecare un danno al giocatore. Il reato si consuma con il conseguimento dell'ingiusto profitto da parte del reo poiché è quello il momento nel quale si viola il diritto del soggetto passivo di disporre del proprio patrimonio. Tale profitto non deve necessariamente essere di tipo patrimoniale, tale da determinare un arricchimento del reo, ma si può anche concretizzare determinando, esclusivamente, una mancata diminuzione del suo patrimonio. Tipico infatti il caso nel quale la frode non porta all'acquisizione di una somma monetaria ma a quella di un servizio. Il reato può essere compiuto esclusivamente con dolo specifico da parte di chi agisce e presenta le stesse pene previste per il reato di truffa.

Delitto di accesso abusivo ad un sistema informatico

L'art.615-ter, va considerato, unitamente al 640 ter, l'articolo più importante introdotto dalla legge n. 547 del 1993 poiché rende penalmente perseguibile l'accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza o il mantenimento in esso contro la volontà espressa o tacita dell'avente diritto. Tale articolo recita:

> Art.615-ter – (Accesso abusivo ad un sistema informatico e 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:
>
> - 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;
> - se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
> - se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
>
> Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque d'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.

Esso, inserito nel capo III del titolo XII del codice penale, è compreso tra i reati contro l'inviolabilità del domicilio in quanto i sistemi violati vengono considerati come una espansione ideale dell'area di rispetto garantita dall'art.14 della Costituzione tutelata dagli articoli 614 e 615bis del codice penale.

Risulta evidente che la definizione di sistema informatico assume una importanza rilevante poiché, nel caso in cui intendessimo come tale l'insieme dei componenti funzionali di un calcolatore e dell'*hardware* ad esso associato la tutela penale espressa nell'articolo sarebbe estesa sia al singolo *personal computer* che al centro di elaborazione dati dotato di *hardware* ben più complesso e sofisticato. Se invece definissimo come tale unicamente una serie di computer in grado di trasmettere dati e segnali tra loro, il singolo PC "*stand alone*" risulterebbe privo di ogni tutela penale. Ciò rappresenterebbe un grave limite poiché un accesso abusivo potrebbe essere operato non solo "da remoto" utilizzando gli strumenti telematici ma anche interagendo sulla tastiera del computer oggetto dell'attacco.

La norma esplicitamente prevede che il sistema informatico o telematico (sistema che integra informatica e telecomunicazioni), perché si configuri il reato in argomento, sia protetto da misure di sicurezza che dimostrino da parte del soggetto avente diritto di non volere consentire l'accesso al sistema alle persone da lui non autorizzate palesando il proprio *ius escludendi*. Ciò implica che accedere ad un sistema a difesa del quale siano state predisposte banali misure di sicurezza come la password "pippo" vada considerata una violazione della norma penale.

Nell'ordinamento penale italiano vengono puniti sia l'"*hacker* buono", cioè colui che viola sistemi informatici per diletto senza fare danni o modifiche, che il "*cracker* cattivo" che danneggia.

Diffusione di computer virus e di apparecchiature dirette a danneggiare o interrompere il funzionamento di un sistema informatico

L'art.615-quinquies, introdotto dalla legge n° 48 del 2008, legge con la quale è stata ratificata in Italia la Convenzione sul *cybercrime* di Budapest, rende penalmente perseguibile la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere il normale funzionamento di un sistema informatico o telematico.

> Art. 615-quinquies – (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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

È stata voluta dal Legislatore la procedibilità di ufficio affinché si possa dare inizio al relativo procedimento penale a carico del reo di tale reato.

I programmi ai quali si fa riferimento in questo articolo sono comunemente conosciuti col nome di *computer virus*. Tali programmi, introdotti in un ambiente informatico, provocano anomalie di funzionamento che possono giungere, nei casi più gravi, alla distruzione totale dei dati ed all'interruzione del funzionamento del sistema. Il Legislatore ha dimostrato particolare attenzione e lungimiranza utilizzando nell'articolo il termine "apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere (il funzionamento di) un sistema informatico" anziché quello di *computer virus*. Infatti, la definizione di *computer virus* è riferibile esclusivamente ad un programma in grado di auto replicarsi (analogamente ai virus biologici). Se fosse stato utilizzato tale termine, non si sarebbe potuta offrire tutela penale nel caso in cui i dati contenuti in un PC fossero stati danneggiati o distrutti da un programma non avente tali caratteristiche, mentre è nota l'esistenza di programmi che comportano tale effetto pur non avendo la capacità di auto replicarsi. Inoltre, con la definizione utilizzata il Legislatore ha voluto essere estremamente generico così da mantenere la norma attuale negli anni. La norma appare attuale poiché sanziona sia la diffusione di *computer virus* a mezzo di dispositivi di memoria portatili che per via telematica, modalità più frequente.

Affinché il reato si compia non è necessario l'effettivo danneggiamento o l'alterazione del funzionamento del sistema informatico poiché, come specificato nell'articolo, è sufficiente che l'apparecchiatura, il dispositivo o il programma informatico siano stati prodotti, diffusi o comunque messi a disposizione con lo scopo di danneggiare il sistema informatico o le informazioni ed i dati in esso contenuti. Si tratta di un così detto reato di pericolo giacché, il verificarsi dell'evento "danneggiamento" è sanzionato, a seconda dei casi, dall'articolo 635 bis (Danneggiamento di informazioni, dati e programmi informatici), dall'articolo 635 ter (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), dall'articolo 635 quater (Danneggiamento di sistemi informatici o telematici) o dall'articolo 635 quinquies (Danneggiamento di sistemi informatici o telematici di pubblica utilità).

Risulta quindi impossibile che si configuri esclusivamente il "tentativo" di diffondere programmi diretti a danneggiare o interrompere il normale funzionamento di un sistema informatico poiché il "tentativo" è definito nel codice penale come il compimento di atti diretti in modo non equivoco a compiere un delitto se l'azione non si compie o l'evento non si verifica. Ne deriva che in presenza di tali atti siamo già di fronte al compimento del reato di cui al 615 quinquies e non semplicemente ad un "tentativo".

Detenzione e la diffusione abusiva di codici di accesso a sistemi informatici

L'articolo 615-quater, introdotto dalla legge n° 547/93, intitolato "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", recita:

> Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a 5164 euro.
>
> La pena è della reclusione da uno a due anni e della multa da 5164 a 10329 euro se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617-quater.

La conoscenza di codici altrui permette di inserirsi abusivamente nei sistemi in argomento e tali codici vengono spesso scambiati tra *hacker*; sempre tra gli *hacker* è consuetudine scambiarsi consigli, quelle "indicazioni e istruzioni idonee" che, a norma dell'art. 615-quater, integrano la fattispecie di reato.

Il reato si configura anche quando l'acquisizione abusiva di codici avviene mediante autonoma elaborazione. È il caso dell'*hacker* che, grazie ad appositi programmi ed alla elevata velocità di elaborazione di un comune PC, riesce, attraverso innumerevoli e ripetuti tentativi, a scoprire codici che consentono l'accesso in sistemi protetti.

Analogamente all'art. 615 ter, relativo all'accesso abusivo ad un sistema informatico, viene offerta tutela penale esclusivamente se vengono riprodotti, diffusi, comunicati o consegnati codici di sistemi informatici protetti da misure di sicurezza.

Il legislatore, non potendo prevedere quali saranno i metodi di autenticazione utilizzati in futuro, ha voluto citare, oltre ai codici ed alle parole chiave, anche "gli altri metodi idonei all'accesso" per non rendere la norma obsoleta in breve tempo.

Assumono quindi rilevanza penale le seguenti condotte:

- Procurarsi codici: qualunque comportamento attuato al fine di venire a conoscenza degli stessi.
- Riprodurre codici: la creazione di una copia digitale o cartacea o comunque in ogni suo aspetto simile al codice, parola chiave o altro strumento utilizzato.
- Diffondere codici: comunicarli ad altre persone.
- Comunicare codici: trasmetterli in qualunque modo, verbale o telematico, che non sia prettamente "materiale".
- Consegnare codici: darli materialmente a mezzo di consegna di un dispositivo di memoria portatile o altro supporto informatico o meno (ad esempio cartaceo) che li contiene.

Affinché si verifichi una violazione della norma, è necessario un dolo specifico da parte di chi agisce, quello di volere procurare a sé o ad altri un profitto o di arrecare ad altri un danno (essenzialmente di natura patrimoniale).

Questo articolo trova ampia applicazione anche nella lotta alla pirateria satellitare, infatti, il modo di operare tipico delle organizzazioni dedite a tale forma di attività è quello di trasmettere e rendere disponibili codici per accedere a programmi a visione condizionata in seguito al pagamento di una somma.

Danneggiamento di sistemi informatici e telematici

L'articolo 9 della Legge 547/93, ha inserito nel codice penale l'articolo 635 bis titolato "Danneggiamento di sistemi informatici e telematici". Successivamente le norme di recepimento sulla Convenzione di Budapest di cui alla Legge n. 48/08, oltre che modificare il titolato del citato articolo in "danneggiamento di informazioni, dati e programmi informatici", hanno introdotto nell'attuale codice penale, nuove ipotesi di reato inserite nel capo I dedicato ai "Delitti contro il patrimonio mediante violenza alle cose o alle persone". Gli articoli introdotti sono:

Art. 635 bis – (Danneggiamento di sistemi informatici e telematici):

> Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da 6 mesi a tre anni. Se ricorre la circostanza di cui al numero 1) dal secondo comma del'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena della reclusione da uno a quattro anni e si procede d'Ufficio.

Art. 635 ter – (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità):

> Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
>
> Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635 quater – (Danneggiamento di sistemi informatici o telematici)

> Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Art. 635 quinquies – (Danneggiamento di sistemi informatici o telematici di pubblica utilità)

> Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Tutte le fattispecie sono aggravate laddove si configurino le circostanze previste dal secondo comma dell'articolo 635 anche se, realisticamente, le ipotesi applicabili risulteranno essere:

- Danneggiamento commesso con violenza alla persona o minaccia.
- Fatto commesso con abuso della qualità di operatore del sistema.

La particolare considerazione della pericolosità sociale insita nel danneggiamento di sistemi informatici e telematici ha fatto sì, invero, che il legislatore abbia previsto che il reato possa essere perseguibile d'ufficio mentre il mero danneggiamento di dati, informazioni e programmi relativi a soggetti privati è punito con la querela della persona offesa. In quest'ultimo caso, occorrerà che il soggetto passivo del fatto illecito si attivi entro tre mesi dalla conoscenza del fatto reato al fine di manifestare la propria volontà a perseguire l'illecito. La nuova normativa ha, inoltre, meglio evidenziato le modalità di "danneggiamento" attraverso cui si configura la fattispecie criminosa includendovi, come già sopra meglio evidenziato, tutta una serie di ipotesi che ampliano, difatti, lo spettro delle fattispecie criminalmente rilevanti.

Alla luce della nuova normativa, inoltre, particolare attenzione è stata dedicata alla soglia di punibilità.

La semplice "condotta" diretta alla commissione del reato, infatti, con eccezione di quanto previsto dall'art. 635 bis, è di per sé già punibile non essendo necessario provare che il comportamento del reo raggiunga lo scopo prefissato, venendo quest'ultimo ad influire solo sulla quantificazione della pena.

Il legislatore anticipa la soglia di punibilità al fine di meglio sottolineare e quindi sanzionare tutta una serie di comportamenti illeciti riscontrati in questi anni.

La previsione di queste nuove forme di reato ha, difatti, annullato qualsivoglia riferimento all'art. 420 del C.P. che faceva riferimento ai reati di "attentati ad impianti di pubblica utilità". Si è scelto volutamente di codificare autonomamente tutti quei comportamenti delittuosi commessi ai danni di "Enti pubblici o, ad essi pertinenti, o comunque di pubblica utilità". È chiaro che l'attuale normativa ha inteso perseguire tutti quei comportamenti illeciti diretti ad arrecare danno ai sistemi informatici o telematici utilizzati "dallo Stato o da altro Enti pubblici".

Phishing

Il *phishing* è attuato attraverso messaggi informatici ingannevoli che portano la vittima a compiere atti a proprio danno senza esserne consapevole. È sanzionabile applicando l'Art. 615 quater (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici) sopra citato perché è ravvisabile la condotta del procurarsi abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico. Qualora l'ignaro utente non inserisca i propri codici di accesso nel modulo contenuto nella pagina *web* fraudolenta si può comunque ipotizzare la commissione del tentato delitto. L'articolo 56 C.P. stabilisce infatti che, chi compie atti idonei, diretti in modo non equivoco a commettere un delitto, risponde di delitto tentato se l'azione non si compie o l'evento non si verifica.

Si configura anche la truffa secondo l'art. 640 se l'autore del reato agisca con dolo specifico atto ad ottenere un ingiusto profitto con danno altrui:

> Chiunque, con artifizi o raggiri, inducendo taluno in errore, 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 51 a 1032 euro.
>
> La pena è della reclusione da uno a cinque anni e della multa da 309 a 1549 euro:
>
> 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;
>
> 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità.
>
> Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.

Se si tratta, come è abituale, di adescamento attraverso una pagina *web* riprodotta da un sito e modificata per ottenere lo scopo di catturare i codici personali della vittima, si può configurare anche una violazione del diritto d'autore secondo l'art. 171 della legge 633/1941, e successive modificazioni.

> È punito con la multa da 51 a 2065 euro chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma :
>
> a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nel regno esemplari prodotti all'estero contrariamente alla legge italiana.

Truffa nel commercio elettronico

Le condotte relative alle truffe perpetrate mediante l'impiego di piattaforme virtuali riconducono ad una serie di tipologie ben definite riassumibili nelle seguenti ipotesi:

- la descrizione di un oggetto nel quale si fa esplicito riferimento a un modello o una marca più pregiata, nel tentativo di ingannare il compratore o comunque di influenzarlo indebitamente
- vendita di un oggetto dichiarando caratteristiche non vere, ad esempio un oggetto in pessime condizioni che viene descritto come "praticamente nuovo"
- mancato recapito della merce legittimante acquistata
- mancato invio di compenso spettante al venditore.

Tali condotte richiamano la fattispecie di reato prevista dall'art. 640 sopra citato.

Il reato di truffa prevede una struttura logica in cui la condotta criminosa si sostanzia nella previsione dell'utilizzo di artifizi (alterazione della realtà) e raggiri (esposizione di menzogne corredate da ragionamenti idonei a ritenerle veritiere).

Nel caso di acquisiti su piattaforme virtuali è verosimile anche la previsione della cosiddetta "Truffa contrattuale" in quanto nella dinamica tra acquirente e venditore si realizza un negozio giuridico, quale manifestazione di volontà delle parti finalizzata ad un risultato concordato a cui l'ordinamento collega effetti di ordine giuridico in linea con quanto desiderato. In tale ipotesi gli artifizi ed i raggiri sono finalizzati ad incidere sul processo di volizione del soggetto passivo al fine di fargli concludere un contratto, sia negli elementi essenziali sia accessori. Sul piano civilistico vi è la possibilità di esperire un'azione di annullamento ex art. 1441 c.c. e seguenti. In altre parole la truffa contrattuale si realizza laddove vi sia un consenso estorto in modo fraudolento per la conclusione ed il contenuto di un contratto che non si sarebbero realizzati laddove vi fosse stata l'esposizione veritiera dei fatti.

Abuso di carte di credito e debito

L'illecito utilizzo di carte di debito e credito nella rete Internet è considerato nel "sentire popolare" il classico esempio di frode informatica. Tuttavia lo stesso non è sanzionato con l'art. 640 ter titolato "Frode informatica" perché nell'illecito utilizzo di carte di credito non si ravvisa l'alterazione di un sistema informatico o l'intervento su dati, informazioni o programmi in esso contenuti, condotte necessarie per la realizzazione della frode informatica.

L'articolo di legge utilizzato per sanzionare l'illecito utilizzo di carte di credito sulla rete Internet è invece il numero 12 della legge 197 del 1991 che recita:

Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante.

> Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 309 a 1549 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

Nel 1991 il legislatore, per fronteggiare il fenomeno connesso all'utilizzo fraudolento delle carte di credito o qualsiasi altro analogo documento che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ha inserito una nuova fattispecie penale (art.12 L.197/91) con l'obiettivo di inasprire le pene per una serie di condotte riferibili all'uso fraudolento delle stesse.

L'applicazione di tale normativa ha consentito agli uffici di Polizia impegnati nel contrasto a tali manifestazioni criminose di ottenere ottimi risultati e scoprire sempre nuove modalità di perpetrazione del reato. La diffusione di Internet e la possibilità di effettuare pagamenti *online* attraverso la carta di credito ha offerto nuovi spazi per coloro che intendono servirsi di tale strumento per compiere illeciti dando vita ad una casistica che ha assunto una crescita notevole. Le truffe per via telematica assumono proprie peculiarità soprattutto se rapportate a quelle perpetrate con i sistemi tradizionali (sempre attraverso l'uso di carte di credito). Una prima caratteristica evidenzia che la media della somma truffata per ogni singola transazione è molto modesta, dell'ordine di qualche decina di euro. Un secondo elemento riguarda la sostanziale stabilità del numero delle truffe commesse con i sistemi tradizionali a fronte di quelle perpetrate via Internet che registrano invece un aumento esponenziale.

Le transazioni di solito avvengono con accrediti a favore di società estere che gestiscono le transazioni *online* per conto di siti web che vendono prevalentemente immagini pornografiche o servizi telematici. In questo caso la compravendita viene effettuata direttamente per via telematica riguardando beni immateriali che non necessitano, pertanto, di essere recapitati presso un indirizzo fisico. Poiché questo genere di reato viene commesso anche in danno di soggetti che non hanno mai usato carte di credito per compiere operazioni *online*, è evidente che i numeri della carta non vengano intercettati mentre viaggiano in Rete, ma che gli autori della truffa ne siano comunque venuti a conoscenza in uno dei seguenti modi:

- agire come *merchant account* cioè offrire un servizio di intermediazione per poi riutilizzare illecitamente i numeri di carta di credito di cui si è entrati in possesso
- aver generato numeri di carta di credito utilizzando generatori software ad hoc
- avere complici all'interno delle strutture finanziarie che si occupano della gestione delle carte di credito.

Si evidenzia che, qualora un soggetto, illecitamente, effettuasse acquisti effettuando pagamenti per mezzo di carta di credito sulla rete Internet semplicemente utilizzando i dati carpiti (numero della carta di credito e data di scadenza), pur non essendo fisicamente in possesso della carta a cui i codici si riferiscono, esso porrebbe in atto due diverse figure di reato: nel momento in cui il soggetto utilizza indebitamente il codice della carta di credito, provocando un danno ingiusto al legittimo titolare, si configura la violazione dell'art. 12 citato mentre, nel momento in cui con l'utilizzo illecito della carta di credito viene perfezionato il contratto di acquisto del bene avremo la violazione dell'art 640 C.P.

Spamming

Lo *spamming* è l'invio di messaggi elettronici non richiesti dal destinatario, a scopo pubblicitario, promozionale o anche solo informativo.

Il Decreto Legislativo 30 giugno 2003 n. 196, noto come "Codice in materia di protezione dei dati personali", permette al destinatario di far valere i seguenti diritti:

Art. 7 titolato" Diritto di accesso ai dati personali ed altri diritti"

> 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
>
> 2. L'interessato ha diritto di ottenere l'indicazione:
>
> a) dell'origine dei dati personali;
>
> b) delle finalità e modalità del trattamento;
>
> c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
>
> d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
>
> e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
>
> 3. L'interessato ha diritto di ottenere:
>
> a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
>
> b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
>
> c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
>
> 4. L'interessato ha diritto di opporsi, in tutto o in parte:
>
> a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
>
> b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il legislatore ha quindi espressamente previsto una prima forma di tutela dell'utente dal fenomeno dello *spamming* introducendo il diritto ad opporsi al trattamento di dati personali effettuato con finalità di invio di materiale pubblicitario o di vendita diretta nonché per il compimento di ricerche di mercato o di comunicazione commerciale.

Tuttavia la forma più intensa di tutela dal citato fenomeno è stata introdotta con l'articolo 130 dello stesso Codice, titolato "Comunicazioni indesiderate". Esso statuisce che:

> 1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24 nonché ai sensi di quanto previsto dal comma 3-bis del presente articolo.

3-bis. In deroga a quanto previsto dall'articolo 129, il trattamento dei dati di cui all'articolo 129, comma 1, mediante l'impiego del telefono per le finalità di cui all'articolo 7, comma 4, lettera b), è consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalità semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale è intestatario in un registro pubblico delle opposizioni.

3-ter. Il registro di cui al comma 3-bis è istituito con decreto del Presidente della Repubblica da adottare ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, previa deliberazione del Consiglio dei ministri, acquisito il parere del Consiglio di Stato e delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, nonché, per i relativi profili di competenza, il parere dell'Autorità per le garanzie nelle comunicazioni, che si esprime entro il medesimo termine, secondo i seguenti criteri e principi generali:

a) attribuzione dell'istituzione e della gestione del registro ad un ente o organismo pubblico titolare di competenze inerenti alla materia;

b) previsione che l'ente o organismo deputato all'istituzione e alla gestione del registro vi provveda con le risorse umane e strumentali di cui dispone o affidandone la realizzazione e la gestione a terzi, che se ne assumono interamente gli oneri finanziari e organizzativi, mediante contratto di servizio, nel rispetto del codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 12 aprile 2006, n. 163. I soggetti che si avvalgono del registro per effettuare le comunicazioni corrispondono tariffe di accesso basate sugli effettivi costi di funzionamento e di manutenzione. Il Ministro dello sviluppo economico, con proprio provvedimento, determina tali tariffe;

c) previsione che le modalità tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale è intestatario secondo modalità semplificate ed anche in via telematica o telefonica;

d) previsione di modalità tecniche di funzionamento e di accesso al registro mediante interrogazioni selettive che non consentano il trasferimento dei dati presenti nel registro stesso, prevedendo il tracciamento delle operazioni compiute e la conservazione dei dati relativi agli accessi;

e) disciplina delle tempistiche e delle modalità dell'iscrizione al registro, senza distinzione di settore di attività o di categoria merceologica, e del relativo aggiornamento, nonché del correlativo periodo massimo di utilizzabilità dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente;

f) obbligo per i soggetti che effettuano trattamenti di dati per le finalità di cui all'articolo 7, comma 4, lettera b), di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilità e sulle modalità di iscrizione nel registro per opporsi a futuri contatti;

g) previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli 23 e 24.

> 3-quater. La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3-bis e sul trattamento dei dati sono attribuiti al Garante
>
> 4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.
>
> 5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.
>
> 6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

Tale articolo, quindi, sostanzialmente vieta, in assenza del consenso dell'interessato, l'utilizzo di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonché l'utilizzo di posta elettronica, telefax, messaggi del tipo MMS o SMS o di altro tipo per effettuare comunicazioni commerciali tese al fine sopra citato. Esso vieta, inoltre, l'utilizzo di identità camuffate o celate nell'invio di comunicazioni commerciali o promozionali o effettuate senza l'indicazione del recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7. Tali diritti, ex art 145, possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante. La tutela prevista è di tipo alternativo giacché il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria così come la presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria. Va infine ricordato che il Legislatore ha previsto, per le più gravi violazioni effettuate nel trattamento dei dati personali, alcune sanzioni penali.

L'articolo 167 infatti, titolato "Trattamento illecito di dati", così recita:

> Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
>
> Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Michele Crudele - 2011-07-24