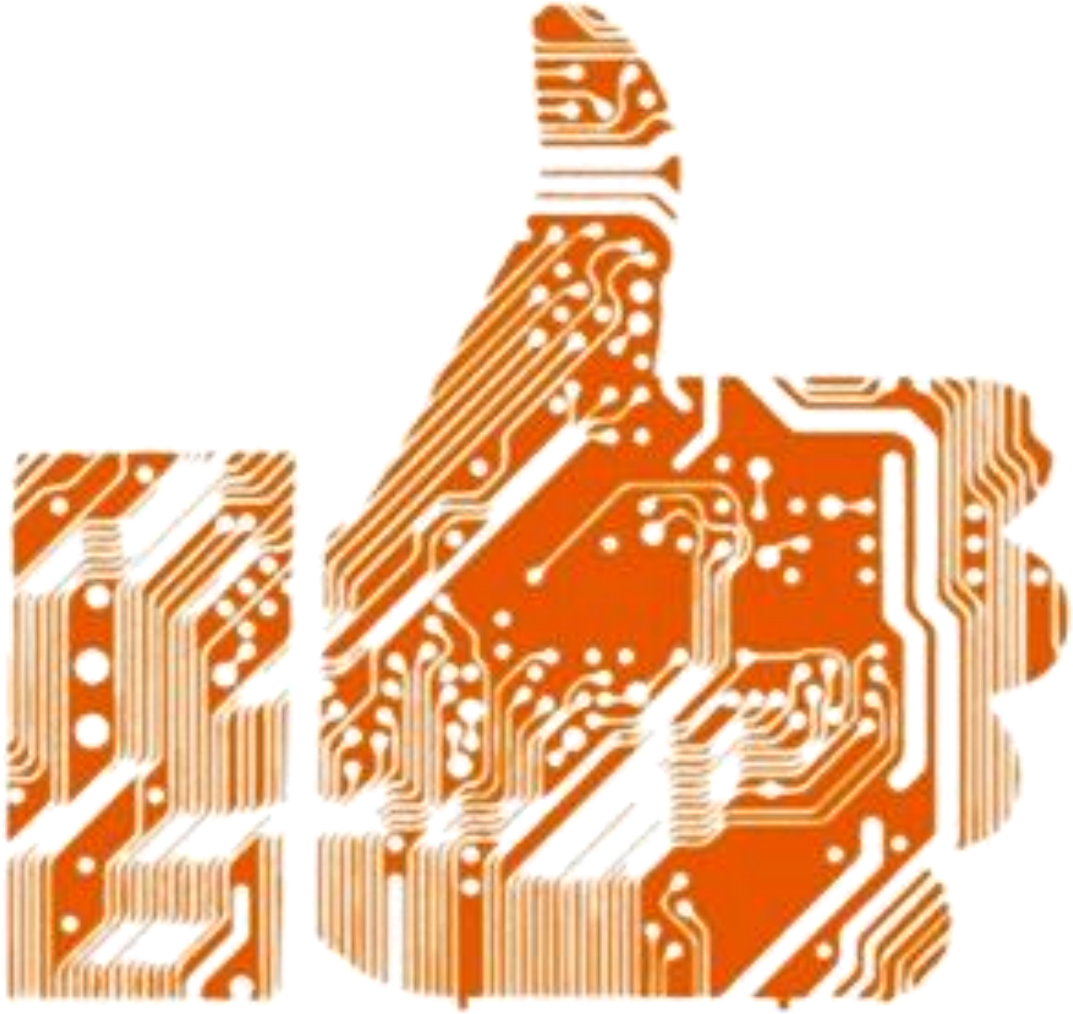
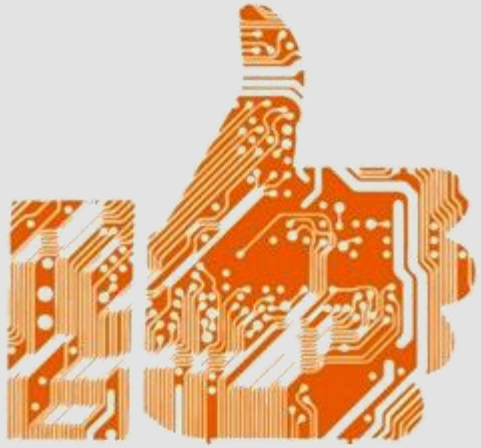


PATENTINO DIGITALE PER ADULTI

Lezione n. 4

I REATI INFORMATICI

Quadro normativo e reati più comuni



I REATI INFORMATICI

AMBITO NORMATIVO

La prima normativa contro i reati informatici (cyber crimes) si rinviene nella legge 547/93 (“modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura procedura penale in tema di criminalità informatica”). A tale norma si aggiungono le modifiche apportate dalla legge 48/2008 avente ad oggetto la ratifica e l'esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, stipulata a Budapest il 23.11.2001.

L'esigenza di perseguire penalmente tali condotte è emersa all'inizio degli anni '90, periodo in cui ha avuto inizio la "migrazione" sulle reti telematiche della maggior parte delle nostre attività lavorative e sociali.

I PIU' COMUNI REATI INFORMATICI

I reati informatici sono disciplinati all'interno del Libro II – Titolo XII del codice penale (delitti contro la persona). Vediamo i più frequenti di seguito.

I REATI INFORMATICI

1. ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO: art. 615 ter c.p. in base al quale *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 in casi particolari in cui, ad esempio, a commettere il fatto sia stato un pubblico ufficiale o un incaricato di un pubblico servizio con abuso di poteri o violazioni di doveri inerenti alla sua funzione o al servizio ovvero se il colpevole, per commettere il fatto ha utilizzato su cose o persone ovvero se dal fatto derivi 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. In questo caso, disciplinato dal secondo comma dell'art. 615 ter c.p., la procedibilità è d'ufficio. In tal caso il luogo di consumazione del delitto coincide con quello in cui si trova l'utente che, tramite elaboratore elettronico o altro dispositivo per il trattamento automatico dei dati, digitando la parola chiave / password, supera le misure di sicurezza apposte dal titolare al fine di selezionare gli accessi.

I REATI INFORMATICI

2.DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI: art. 615 quater c.p.: 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 a un anno e con la multa sino a euro 5.164.

Tale fattispecie si differenzia dalla precedente in quanto prevede l'espressa detenzione e successiva diffusione abusiva di qualunque mezzo idoneo ad accedere a un sistema informatico o telematico protetto da misure di sicurezza.

I REATI INFORMATICI

3. DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO, art. 615 quinquies c.p.: 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.

4.FRODE INFORMATICA, art. 640 ter c.p.: Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

I REATI INFORMATICI

5.DIFFUSIONE ILLECITA DI IMMAGINI O VIDEO SESSUALMENTE ESPLICITI, art. 612 ter c.p.: Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la relcusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000.

La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento.

La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici.

La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi.

I REATI INFORMATICI

Tale fattispecie criminosa, introdotta con la L. n. 69 del 10.07.2019 (Codice Rosso) è comunemente conosciuta come *revenge porn* e attualmente è molto diffusa visto il largo utilizzo dei social network.

IL *REVENGE PORN*, definito anche come «pornografia non consensuale» ed anche abuso sessuale tramite immagini, è l'atto di condivisione di immagini o video intimi di una persona senza il suo consenso, attuato sia *on-line* che *off-line*.

Il punto di partenza del «revenge porn» è il materiale pornografico che rappresenta la vittima in situazioni private e/o intime, sia da sola che con il partner.

I REATI INFORMATICI

Da un punto di vista criminologico ci troviamo di fronte ad una forma avanzata di *cyberbullisimo* e il materiale pornografico può essere carpito in diversi modi:

- **mediante il cosiddetto *sexting*** ovvero l'auto ripresa di immagini o video in pose intime da parte della vittima e successivamente inviate a terzi, anche mediante web cam;

- **mediante la ripresa delle immagini intime** durante un rapporto sessuale con il consenso della vittima;

- **mediante la ripresa della vittima durante momenti intimi** (rapporto sessuale, bagni pubblici, spogliatoi ecc..) con telecamere nascoste (*spy cam*);

- **attraverso l'*hacking* dello spazio cloud della vittima** (icloud, gmail, microsoft space, ecc..) ovvero del dispositivo (smartphone, laptop, smartpad) anche con la consegna spontanea del dispositivo (es. invio di un pc o di un telefono in assistenza);

I REATI INFORMATICI

- tramite *grooming* che consiste nell'adescamento di un minore in Internet tramite tecniche di manipolazione psicologica volte a superarne le resistenze e a ottenerne la fiducia per abusarne sessualmente.

La norma art. 612 ter c.p. Introduce, al primo e la secondo comma, due fattispecie di reato diverse.

Dal punto di vista soggettivo, si tratta di un reato comune e a **dolo generico**.

Invece,**dal punto di vista materiale, gli elementi costitutivi del reato richiedono una progressione fattuale ben circoscritta**.

I REATI INFORMATICI

La condotta tipica è composta, in primo luogo, da **un antefatto anche non punibile** (salvi i casi di interferenza illecita nella vita privata di cui all'art. 615 bis c.p., tanto per fare un esempio), ossia la realizzazione o la sottrazione di immagini o video dal contenuto sessualmente esplicito e la successiva pubblicazione o diffusione dello stesso;**il fatto, per essere rilevante, deve avere per oggetto materiale che doveva** rimanere privato e diffuso «senza il consenso delle persone rappresentate». **Il conseguente invio** (per posta ordinaria, email, sistemi di messaggistica istantenaea ecc,), consegna materiale, cessione, pubblicazione (su social, siti, blog) o diffusione (cioè comunicazione ad un numero indeterminato di persone) **fa scattare la punibilità**.

L'aspetto più problematico riguarda il consenso**:** come deve essere dato (a patto che la persona ritratta voglia astrattamente darlo)? Ciò appare dirimente soprattutto quando l'imputato assuma di essere stato **autorizzato all'invio del materiale (magari ad una cerchia di persone) dal partner** che, vedendo poi diffuso in rete il video, sporga querela.

I REATI INFORMATICI

Il consenso, difatti, può essere esplicito, implicito, tacito (accettazione passiva alla ripresa ed alla successiva comunicazione), prestato oralmente o per iscritto.

Inoltre vanno elencati eventuali vizi del consenso in relaziona alla:

•Capacità(minore età, interdizione o inabilitazione, causa temporanea per malattia, infortunio, abuso di sostanze alcoliche o stupefacenti);

•Libertà(errore, violenza, dolo – art. 1427 c.c.);

•Consapevolezza (scopo della raccolta del dato, limiti alla sua comunicazione o diffusione).

Inoltre, ipotizzando che il consenso della persona offesa sia stato dato, è possibile per la stessa revocarlo dopo la diffusione, anche massiva del materiale di sua pertinenza?

O meglio, una volta che il consenso è stato revocato, sarebbe possibile per la persona offesa decidere se un fatto possa costituire reato, magari eludendo i termini per la querela, oppure ciò rileverebbe solo ai fini civilistici?

I REATI INFORMATICI

Ed appare evidente che, se si sposta l'attenzione dalla persona offesa verso l'imputato,lo stesso avrà un onere abbastanza gravoso nel dover dimostrare di essere stato autorizzato alla comunicazione, diffusione ovvero ad una sola di queste facoltà, operando, come sembra, una presunzione iuris tantum in favore della vittima: la regola è che tutto ciò che è fatto nell'intimità, ancorché consapevolmente, deve rimanere riservato,salvo prova contraria.

Oltretutto la norma punisce anche chi sottrae il materiale de quo (si pensi al furto di un telefono, oppure al caso dei PC portati in assistenza e trafugati da tecnici poco seri, ovvero in caso di accesso abusivo ai propri dati).

In ogni caso solo l'applicazione concreta della norma potrà sciogliere tali dubbi interpretativi, sulla scorta, soprattutto, di una prognosi postuma che il giudice deve fare all'atto della valutazione di indici esteriori quali la condotta dell'imputato prima e dopo il fatto, la tempistica fra produzione e comunicazione e diffusione, la presenza di correi...

I REATI INFORMATICI

Il secondo comma dell'art. 612 ter c.p. punisce invece chi riceve o acquisisce il materiale intimo e pone in essere le condotte del primo comma senza il consenso delle persone riprese al fine di recare loro nocumento.

Il dolo, difatti, è specifico in quanto l'agente deve essere consapevole, oltre di stare ponendo in essere la condotta tipica, di rappresentare l'ulteriore scopo di arrecare un danno (all'immagine, alla salute, al patrimonio) al di là della realizzazione dello stesso.

Anche qui, dal punto di vista processuale, siamo di fronte ad una probatio diabolica **in quanto l'agente dovrà dimostrare di avere concorso nella diffusione senza voler danneggiare nessuno.**

Sembrerebbe, inoltre, che il consenso richiesto sia ulteriore e diverso rispetto a quello dato per le riprese o per una comunicazione "limitata" delle immagini, pertanto emergono, anche in questa sede, le medesime problematiche interpretative sopra esposte.

Per quanto riguarda le circostanze aggravanti, il terzo comma prevede un'aggravante se **i fatti sono stati commessi da persone che hanno o hanno avuto legami affettivi con la vittima** e se sono commessi mediante strumenti informatici o telematici (ossia nella quasi totalità dei casi).

I REATI INFORMATICI

Si prevede poi una circostanza ad effetto speciale (da un terzo sino alla metà) qualora la vittima versi in stato di **inferiorità psichica o fisica ovvero sia una donna in stato di gravidanza**.

Le predette circostanze aggravanti sono coerenti con il maggior disvalore penalistico in ragione della qualità della persona offesa e con penetrante incisività del mezzo utilizzato.

L'ultimo comma disciplina la condizione di procedibilità che, in coerenza anche sistematica con il precedente art. 612 bis **(*stalking***), è la querela ma entro mesi sei dalla conoscenza del fatto.

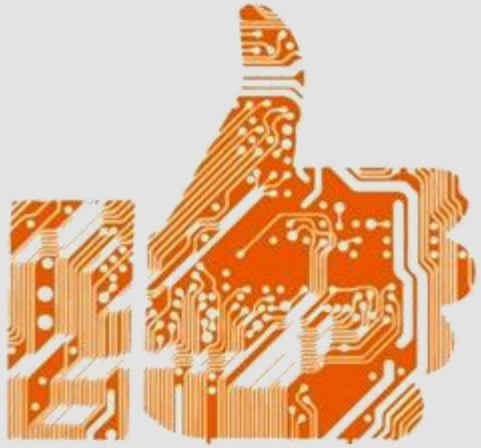
Si procede d'ufficio in caso di fatti previsto al quarto comma (aggravanti speciali) e qualora vi sia connessione con un reato più grave.

Tutte le fattispecie di reato sopra descritte sono accomunate da un problema di carattere processuale, ossia dalla difficoltà di individuare il giudice competente, alla stregua del criterio indicato dall'articolo 8 comma 1 c.p.p., il quale dispone, come regola generale, la competenza del giudice del luogo nel quale il reato si è consumato; tale problema nasce in quanto vi sono dei reati, cosi come nel caso dei cyber crimes, nel quale è impossibile risalire a quel luogo.

I REATI INFORMATICI

Con riferimento al luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico di cui all'articolo 615 ter c.p., le Sezioni Unite della Corte di Cassazione con la sentenza del 26 marzo 2015 n. 17325 ha risolto il contrasto disponendo che: "*il luogo di consumazione del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-ter c.p., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente*". La regola della competenza radicata nel luogo dove si trova il soggetto commissivo dell'introduzione abusiva ad un sistema informatico o telematico, non trova eccezioni per le forme aggravate del reato in esame. Ad un'analoga conclusione si perviene anche con riguardo alle condotte di mantenimento nel sistema informatico contro la volontà di chi ha diritto di escluderlo ex articolo 615 ter c.p., mentre nelle ipotesi meramente residuali in cui non risulta rintracciabile la piattaforma su cui ha operato si applicheranno i criteri tracciati dall'articolo 9 c.p.p.

RESPONSABILITA' GENITORIALI E PERSONALI SUL WEB



RESPONSABILITA' GENITORIALI E PERSONALI SUL WEB

RESPONSBABILITA' GENITORIALI E PERSONALI SUL WEB

Ad oggi non esiste una disciplina generale e uniforme del consenso digitale del minore. Il legislatore europeo e quello italiano sono intervenuti solo in tema di trattamento dei dati personali del minore.

La materia è dunque attualmente disciplinata dal Regolamento Europeo n. 679/2016 che prevede quanto segue: “il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un’età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale”.

La normativa lascia tuttavia agli Stati la possibilità di stabilire un’età diversa, purché non inferiore a tredici anni (articolo 8). L’Italia ha fissato in 14 anni l’età minima (articolo 2-quinquies, decreto legislativo n. 101/2018), così disattendendo il parere dell’Autorità garante per l’infanzia e l’adolescenza, che riteneva necessario evitare di “porre in capo a ragazze e ragazzi con meno di 16 anni il dovere di essere consapevoli circa le conseguenze del consenso al trattamento dei dati personali” in quanto ciò significherebbe “caricarli di un onere conoscitivo e di comprensione gravoso” (cfr. parere prot. n. 0001008/2018 del 24 aprile 2018).

RESPONSABILITA' GENITORIALI E PERSONALI SUL WEB

Il nostro ordinamento prevede varie ipotesi in cui il minore è in grado di assumere talune responsabilità di carattere civile (si veda, ad esempio: al compimento del sedicesimo anno d'età termina l'obbligo scolastico e il minore può far ingresso nel mondo del lavoro – articolo 3, legge n. 977/1967 e s.m.i.; previa autorizzazione, il sedicenne può contrarre matrimonio – articolo 84, comma 2, c.c., e riconoscere un figlio – articolo 250, ultimo comma, c.c.) e assumere autonomamente scelte essenziali per il suo sviluppo (ad esempio: il minore ultraquattordicenne deve manifestare il consenso all'adozione nei confronti della coppia prescelta dal tribunale per i minorenni – articolo 25, comma 1, legge n. 184/1983; il minore di qualsiasi età capace di discernimento può richiedere personalmente trattamenti sanitari – articolo 120, d.p.r. n. 309/1990 sulla tossicodipendenza – o rifiutarli).

RESPONSABILITA' GENITORIALI E PERSONALI SUL WEB

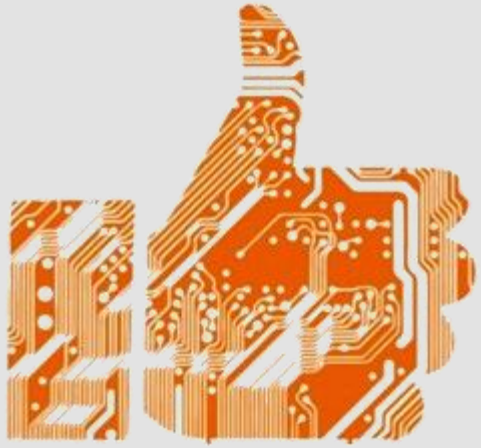
Rispetto al tema qui analizzato, considerando che l'ingresso dei minori nel mondo digitale avviene ben prima dei sedici anni, il legislatore ha scelto di abbassare a quattordici anni l'età per il consenso al trattamento dei dati personali al fine di favorire una responsabilizzazione dei minori, tenuto conto anche che la stessa legge contro il cyberbullismo consente al minore ultraquattordicenne di agire personalmente a tutela della propria dignità e della c.d. identità digitale (art. 2 L. n. 71/2017). Quest'ultima norma ha fornito, per la prima volta, una definizione giuridica del *cyberbullismo* inteso come (cfr. art. 1) qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo. e indica misure di carattere preventivo ed educativo nei confronti dei minori (qualunque sia il ruolo nell'episodio) da attuare in ambito scolastico, e non solo.

RESPONSABILITA' GENITORIALI E PERSONALI SUL WEB

Ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella rete. Se entro 24 il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore. Il Garante ha peraltro pubblicato nel proprio sito il modello per la segnalazione/reclamo in materia di cyberbullismo da inviare a: cyberbullismo@gpdp.it.

È stata estesa al cyberbullismo la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.). In caso di condotte di diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minorenne, se non c'è stata querela o non è stata presentata denuncia, è applicabile la procedura di ammonimento da parte del Questore (il questore convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale). Gli effetti dell'ammonimento cessano al compimento della maggiore età.

PRIVACY ONLINE



PRIVACY ONLINE

Il Comitato europeo per la protezione dei dati (organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione) col nuovo Regolamento Europeo ha sostituito il Gruppo di lavoro articolo 29 (Working Party article 29o WP29, appunto perchè previsto dall'art. 29 della direttiva europea 95/46), ed è il gruppo di lavoro comune delle Autorità nazionali di vigilanza e protezione dei dati. Le linee guida sul consenso adottate dal WP29, peraltro, riportano alcune indicazioni a completamento delle disposizioni del GDPR in tema di modalità di raccolta del consenso informato di un minore: il titolare del trattamento deve utilizzare un linguaggio chiaro e semplice, comprensibile per i minori, per informarlo di come intende trattare i dati raccolti, nonché adottare “ogni ragionevole sforzo per verificare che l’utente abbia raggiunto l’età del consenso digitale”, in considerazione del tipo di trattamento operato e dei rischi connessi.

PRIVACY ONLINE

Un profilo parallelo alla liceità del trattamento dei dati del minore rispetto ai servizi web – che presuppone quindi il consenso del minore ultraquattordicenne o il consenso dei genitori se di età inferiore – è quello relativo al dovere di controllo dei genitori (o di chi esercita la responsabilità genitoriale) sul modo in cui i minori utilizzano il web. Da un lato, i genitori hanno il diritto-dovere educare i figli; dall'altro, "sono responsabili del danno cagionato dal fatto illecito dei figli minori" (articolo 2048, comma 1, c.c.), il che li obbliga a un preciso dovere di vigilanza, diretto sia a impedire che i minori possano subire pregiudizi, sia a prevenire il pericolo che i minori stessi ne arrechino a terzi (v. cyberbullismo). Non a caso, la giurisprudenza ha già sperimentato forme di controllo della responsabilità genitoriale in presenza di rischi derivanti dall'uso di social network e la dottrina, da tempo, riflette su come adattare o innovare le regole della responsabilità civile al mondo digitale.

Grazie per l'attenzione!

ADOC Toscana APS

Via Vittorio Corcos, 15 – 50142 Firenze (FI)
Tel./Fax 055 7325586 - adoctoscana@gmail.com