INFORMATION TECHNOLOGY LAW

DISPENSE

(Ignazio Zangara)

… … …

SEZIONE V
CRIMINI INFORMATICI

INTRODUZIONE

Come tutti i fenomeni sociali anche la criminalità ha trovato terreno fertile nel mondo della rete. I crimini informatici o computer related crimes si sono moltiplicati a dismisura negli ultimi vent'anni.

Il legislatore italiano, di volta in volta, ha adeguato l'ordinamento giuridico pubblicando leggi speciali per garantire la tutela ed il rispetto dei beni giuridici protetti e dei valori essenziali minacciati attraverso l'utilizzo di strumenti informatici; gli interventi normativi non sono stati coordinati, si è intervenuto a singhiozzo, a macchia di leopardo, colmando ora da un lato ora da un altro le lacune legislative.

Il ricorso al diritto penale per la tutela dei valori fondamentali su cui lo Stato si fonda, lo si è detto nella prima sezione di queste dispense, rimane, tuttavia, una *extrema ratio*, poiché per le violazioni più lievi deve applicarsi la disciplina di diritto civile o amministrativo che impattano meno violentemente sulla dignità dell'uomo.

I valori più alti che lo Stato tutela attraverso l'ordinamento giuridico penale sono, in via esemplificativa, la vita e l'integrità fisica/morale/psicologica, la salute, il patrimonio dei singoli e dello Stato, l'integrità dello Stato e delle istituzioni, l'ordine pubblico, la fede pubblica, ecc.

PREMESSE NORMATIVE E PRINCIPIO DI LEGALITÀ

In considerazione della gravità dell'intervento penale nella repressione delle condotte illecite, il processo di evoluzione che ha condotto ad un sistema giuridico penale garante dei diritti dei suoi consociati può farsi risalire al 1789 con la 'Dichiarazione dei diritti dell'uomo e del cittadino' in cui venne riconosciuto il principio cardine dei moderni sistemi giuridici penali, che prevede il divieto di irretroattività della legge penale. Esso si configura quale corollario della divisione dei poteri nello Stato di diritto. Tale principio fu riferito, in un primo momento, soltanto alla sanzione, più che alle regole di comportamento, al fine di limitare l'arbitrarietà dell'applicazione delle misure coercitive che possono giungere anche a limitare la libertà di un individuo. Subito dopo, il principio fu esteso alla previsione normativa vera e propria, cioè alla prescrizione della fattispecie di reato. Fu nei primi anni dell'Ottocento che un noto criminalista tedesco, Anselm Feuerbach, affermò il postulato *Nulla poena sine lege*, che presto fu raccordato concettualmente al principio di prevenzione generale del precetto penale attuato mediante la coazione psicologica. In altri termini, la minaccia della pena, indicata nelle fattispecie di reato, funge da deterrente psicologico e distoglie i consociati dal commettere reati; perché ciò possa verificarsi, quindi, è necessario che i consociati conoscano prima quali sono i fatti (azioni od omissioni) la cui realizzazione o compimento comporta l'inflizione della sanzione penale.

In Italia il principio in parola è sancito all'art. 25, secondo comma, della Carta costituzionale, che recita: "Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso". Il medesimo principio è stato ribadito all'art. 7 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma nel 1950.

Il diritto penale in Italia è governato dal 'principio di legalità' che a sua volta si declina su quattro direttive: 1) la riserva di legge. Lo Stato riserva la potestà normativa in materia penale al legislatore ordinario, cioè al Parlamento che rappresenta la volontà del popolo. Ciò trova giustificazione nelle esigenze di garanzia che il procedimento legislativo ordinario assicura. Infatti,

solo con i passaggi, le verifiche e i controlli previsti nel procedimento legislativo ordinario si possono tutelare e salvaguardare gli interessi fondamentali di tutti i consociati, senza rischiare disparità di trattamento o derive maggioritarie; esso consente l'intervento, durante l'iter di formazione delle leggi, delle minoranze, dell'opposizione, di tutti i portatori di interessi al fine di approvare testi equi e ponderati. Le fonti di rango secondario possono dare un apporto normativo di tipo tecnico, partecipando alla specificazione di disposizioni di rango primario (si pensi al settore della sanità, dove continuamente sono aggiornate le tabelle ministeriali che stabiliscono quali sostanze sono da considerare stupefacenti); 2) la tassatività o sufficiente determinatezza della fattispecie penale. Il legislatore deve individuare con un certo grado di precisione qual è il comportamento penalmente sanzionato. Il consociato deve sapere con esattezza quale condotta non può tenere e cosa gli è invece consentito fare, qual è il confine tra il lecito e l'illecito. La determinatezza della fattispecie penale è stata prevista per evitare che il compito di stabilire se un comportamento sia lecito o illecito finisca per essere sbilanciato, concedendo alla Magistratura un peso eccessivo; 3) l'irretroattività della legge penale. Consiste nel divieto di applicare la legge penale a fatti commessi prima della sua entrata in vigore. Il principio è in effetti valido per tutte le leggi dello Stato, ai sensi di una regola generale secondo cui la legge non dispone che per l'avvenire. In diritto penale tale principio è applicato con assoluto rigore, laddove in altri ambiti del diritto, talvolta, si opta per soluzioni più flessibili. In tal senso, tuttavia, esiste un'eccezione che si applica anche al rigore penale nei casi in cui una norma più favorevole può essere applicata ad un fatto commesso prima della sua entrata in vigore. In altri termini, in ambito penale se in un determinato momento una legge (o una pronuncia della Corte Costituzionale) dovesse ridurre la misura della pena o perfino depenalizzare un comportamento o un fatto che fino a quel momento era previsto come reato, chiunque sia incorso in quella fattispecie non sarà più punito con quanto era previsto dalla legge penale al momento in cui il fatto è stato commesso. Quindi, anche se il fatto era considerato reato al momento della sua commissione, l'entrata in vigore di una legge (o la pubblicazione di una sentenza della Corte Costituzionale) meno rigorosa dovrà applicarsi al reo, cioè a colui che ha commesso l'illecito. Sarebbe, infatti, incongruo infliggere una pena ad un soggetto per un fatto che oggi non è più previsto come reato o infliggere una pena più grave rispetto a quella prevista dalle norme vigenti. Questo principio, detto del *favor rei*, intende evitare di punire un soggetto per un fatto che al momento in cui è stato commesso prevedeva una conseguenza più rigorosa rispetto al momento in cui si celebra il processo o viene eseguita la pena. L'ordinamento, in questi casi, ritiene quella condotta meno grave rispetto alla salvaguardia degli interessi e dei valori fondamentali tutelati dall'ordinamento penale. Si pensi all'adulterio femminile che prima del 1968 costituiva una fattispecie di reato e, grazie ad una sentenza della Corte costituzionale, la fattispecie fu depenalizzata. Quindi se oggi si scoprisse che prima di quella data una donna tradì il marito, non si applicherà alla stessa alcuna norma o sanzione penale, proprio perché il comportamento, tenuto all'epoca, non ha oggi alcun disvalore penale. Analogamente, se una riforma di una norma penale rendesse meno severa una sanzione per un fatto di reato, il soggetto responsabile subirà la condanna meno grave anche se ha commesso il reato prima della riforma; 4) il divieto di analogia in materia penale. L'analogia è un processo di integrazione dell'ordinamento che consente al giudice, in assenza di una norma specifica che regoli la fattispecie su cui è chiamato a decidere, di applicarne una che regoli casi o materie analoghe. L'ordinamento giuridico, in virtù del principio *ubi eadem ratio ibi eadem legis dispositio*, consente al giudice di colmare lacune normative e di risolvere le questioni interpretando le norme e applicando un criterio certo. L'analogia, dunque, proprio per la sua caratteristica di estensività della precetto normativo, non opera in ambito penale perché sarebbe in palese contrasto con la tassatività della fattispecie penale, sopra descritta.

NOZIONI GENERALI DI DIRITTO PENALE

Il diritto penale è caratterizzato da una serie di termini e di concetti specifici che è opportuno chiarire prima di analizzare le singole fattispecie di reato.

Costituisce un illecito qualunque comportamento antigiuridico, sia di diritto pubblico che di diritto privato. L'illecito penale è rappresentato da una fattispecie di reato, cioè da un fatto che dipende dall'operato dell'uomo, anche di natura omissiva, al quale l'ordinamento giuridico ricollega una sanzione penale.

La responsabilità penale è personale, cioè non è trasmissibile a nessun altro. In altri termini, l'ordinamento penale può comminare pene soltanto all'autore del reato, salvo il caso della responsabilità oggettiva di cui si dirà più avanti.

In qualunque caso, l'ordinamento italiano garantisce al soggetto incriminato il diritto di difesa in ogni ordine (davanti a qualunque giudice) e grado (di merito e di legittimità) di giudizio. La difesa è un diritto inviolabile sancito dalla Costituzione e prevede che chiunque possa difendersi in giudizio per tutelare la propria posizione giuridica in merito ad un fatto illecito, anche se indigente, tramite l'istituto del gratuito patrocinio[1].

Nella maggior parte delle fattispecie di reato vi è un soggetto attivo (o soggetto agente) cioè colui che commette il reato ed un soggetto passivo cioè colui che subisce o patisce le conseguenze dell'azione criminosa. Il soggetto passivo può essere anche diverso dall'individuo, come ad esempio un'istituzione quale lo Stato, un'università, un'impresa, la collettività nel suo complesso, ecc. Il soggetto attivo è sempre un individuo che risponde del proprio comportamento. Nei casi in cui un fatto sia attribuibile ad un ente, un'associazione, un'impresa la responsabilità penale ricade nella persona che ne ha la rappresentanza legale.

Vi sono reati che sono perseguiti dallo Stato in automatico, ossia lo Stato attiva la procedura di accertamento di quanto accaduto nel momento in cui viene a conoscenza della notizia di reato. Questo accade nei casi in cui vengono commessi i reati più gravi per cui si procede appunto d'ufficio. In altri casi, per poter attivare la tutela penale prevista dall'ordinamento, non è sufficiente ricevere la notizia del reato, ma è necessario un atto formale, che prende il nome di querela, da parte dell'offeso dal reato. Si richiede quindi un'istanza di parte come condizione di procedibilità per i reati meno gravi, quali ad esempio la minaccia o la diffamazione. L'azione penale ed il processo scaturiscono solo se viene sporta la querela da parte di chi ha subito le conseguenze del fatto delittuoso.

Alcuni comportamenti criminosi possono essere compiuti da chiunque: si pensi all'omicidio, al furto, all'omissione di soccorso. Si tratta dei c.d. reati comuni[2]; altri reati, invece, possono essere commessi soltanto da individui che ricoprono una particolare posizione giuridica, come ad esempio un funzionario pubblico, la madre, il marito, il testimone. Sono i c.d. reati propri[3], per i quali la legge prevede una pena più severa rispetto a quella comminata ad un *quisque de populo* (un comune consociato) per una condotta identica. Per continuare con gli esempi di cui sopra, si pensi al furto di un bene dell'amministrazione pubblica da parte di un impiegato pubblico, all'infanticidio, all'uxoricidio, alla falsa testimonianza.

---

[1] Il gratuito patrocinio o patrocinio a spese dello Stato consente ad un soggetto non abbiente di ottenere il pagamento da parte dello Stato della parcella dell'avvocato difensore.

[2] Gli artt. 392 e 393 del c.p. prevedono, ad esempio, i reati comuni di esercizio arbitrario delle proprie ragioni con violenza sulle cose o alle persone, con l'obiettivo di punire chi intenda di farsi giustizia da sé senza ricorrere alla magistratura o, in generale, ai mezzi messi a disposizione dallo Stato.

[3] Costituiscono esempi di reati propri: il Peculato (art. 314 c.p.) "Il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di danaro o di altra cosa mobile altrui, se ne appropria … anche temporaneamente …"; la Concussione (art. 317 c.p.) "Il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità …"; la Corruzione (art. 318 c.p.) "Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa …".

In tutti i casi, la pena a chiunque comminata, nell'ordinamento italiano, deve tendere alla rieducazione del condannato, in una visione di recupero e valorizzazione della persona umana e non di umiliazione e abbandono.

Alcune fattispecie di reato prevedono una soglia di punibilità molto bassa; si tratta dei c.d. 'reati di pericolo', per i quali la condotta criminosa si perfeziona con la semplice messa in pericolo o lesione potenziale del bene oggetto della tutela penale. Nella maggior parte dei casi, invece, il perfezionamento della fattispecie di reato avviene con la lesione effettiva del bene protetto. Questi ultimi sono detti 'reati di evento. Per il primo caso, si pensi ad un soggetto che detenga illegalmente armi e, per il secondo caso, al sequestro di persona.

Ai fini del perfezionamento del reato, in generale, è necessario valutare l'elemento psicologico del soggetto agente. Infatti, la fattispecie criminosa prevede, nella maggior parte dei casi, che la condotta da parte del soggetto agente sia compiuta intenzionalmente. Il dolo è l'elemento psicologico che il giudice deve ricercare nel soggetto incriminato per poter infliggere la pena.

Il dolo si configura, dunque, allorquando il soggetto agente con la sua condotta criminosa ha preveduto e voluto il verificarsi dell'evento dannoso o pericoloso a danno del bene protetto.

In altri casi, quando è espressamente previsto dalla norma di diritto penale, l'agente risponde anche quando con la sua condotta, pur potendolo prevedere, non ha voluto il verificarsi dell'evento dannoso che si verifica a causa di negligenza, imprudenza, imperizia, per inosservanza delle leggi, ordini o discipline. È il caso della responsabilità per colpa. Per il primo caso, si pensi all'omicidio volontario di colui che spara per uccidere il rivale in amore e, per il secondo caso, all'omicidio stradale di colui che – non osservando le norme del codice della strada o, in generale, di prudenza alla guida – sbanda con l'automobile e uccide un pedone.

Come può facilmente intuirsi, ciascuna fattispecie di reato prevista in astratto dal legislatore, può verificarsi arricchita da elementi particolari che rendono unica, o quasi, la fattispecie concreta. Si tratta delle cosiddette 'circostanze del reato' che possono causare l'aumento o la diminuzione della misura della pena da infliggere perché il disvalore sociale è più o meno marcato. Per le prime, si parla di 'circostanze aggravanti', come la commissione del reato per celarne un altro già commesso, la commissione del reato ai danni di un minore, la particolare efferatezza nella commissione dell'omicidio, la recidiva, cioè la ripetizione di una condotta criminosa per la quale si era già subito un processo, ecc. Per le seconde, le cosiddette 'circostanze attenuanti', si pensi, ad esempio, ai casi in cui la condotta criminosa cagiona un danno di lieve entità, o quando il soggetto agente ripara il danno prodotto prima del giudizio, ecc.

Infine, un cenno deve farsi sulle 'circostanze esimenti', altrimenti dette 'scriminanti' o 'cause di giustificazione', in presenza delle quali la condotta, che in astratto configura un reato, in concreto non è ritenuta antigiuridica. Le esimenti sono lo 'stato di necessità', l''esercizio di un diritto o l'adempimento di un dovere', la 'legittima difesa'. Lo stato di necessità esclude, ad esempio, la fattispecie di furto quando un soggetto, non potendo fare altrimenti, ruba un'auto per portare sé o altri ad un pronto soccorso in caso di imminente pericolo di vita. L'esercizio di un diritto o l'adempimento di un dovere escludono, rispettivamente, la diffamazione a mezzo stampa da parte di un giornalista che esercita il diritto di cronaca raccontando la verità sui fatti commessi da un soggetto oppure l'omicidio quando un cecchino riceve l'ordine del suo superiore di fare fuoco ed uccidere il terrorista che sta per innescare un ordigno tra la folla. La legittima difesa esclude, ad esempio, il reato di lesioni personali ai danni di un soggetto quando quest'ultimo minaccia concretamente l'integrità fisica del soggetto agente, purché l'azione a difesa sia proporzionata alla minaccia ricevuta.

Per i fatti di reato l'ordinamento penale prevede pene pecuniarie e pene detentive. Senza approfondire in questa sede, le prime sono la multa e l'ammenda e le seconde sono l'ergastolo, la reclusione e l'arresto.

CRIMINI INFORMATICI

Viste per sommi capi le caratteristiche di ordine generale dell'ordinamento penale italiano, nelle prossime pagine saranno esaminati alcuni dei principali crimini informatici. Sotto quest'ultima denominazione, gli studiosi a livello concettuale distinguono i reati commessi per mezzo dell'elaboratore elettronico e dei programmi in esso installati (dove il computer è lo strumento attraverso il quale la condotta criminosa viene posta in essere) dai reati commessi a danno degli elaboratori, dei programmi e dei dati in essi contenuti (dove l'azione criminosa è volta a compromettere il corretto funzionamento e l'integrità di un sistema elettronico in senso ampio). Spessissimo le due categorie finiscono per mescolarsi e accade che lo strumento informatico viene utilizzato per compromette un sistema informatico o il corretto funzionamento di un programma o l'integrità di un dato informatico. In altri casi, l'uso criminale dell'elaboratore può incidere in maniera diretta sui beni reali (si pensi alla manomissione di un sistema elettronico di erogazione di banconote per appropriarsi di denaro contante).

Una parte di dottrina sostiene che si sta sviluppando un terzo genere di crimini informatici in cui il soggetto agente è proprio il sistema informatico. Le ipotesi, che sfociano nel fenomeno dilagante dell'intelligenza artificiale avanzata, potrebbero farsi rientrare negli ambiti tradizionali della responsabilità oggettiva, cioè in fattispecie di reato colposi (i casi, ad esempio, di *culpa in vigilando*) per i quali un soggetto risponde per l'operato di altri[4], ma trattandosi di una realtà in divenire, non si può escludere che nei prossimi anni si configuri una disciplina *ad hoc* per i fatti di reato commessi da sistemi esperti, agenti intelligenti e altre realtà virtuali avanzate che operano nelle reti.

Nella maggior parte dei casi, il legislatore penale italiano, così com'è avvenuto in Germania, nel corso del tempo ha inserito i nuovi reati informatici all'interno del codice penale ed è intervenuto in maniera organica (i tecnici parlano, per l'appunto, di intervento ortopedico), affiancando alle fattispecie di reato reali quelle corrispondenti o analoghe di tipo informatico. Così, troviamo di seguito al reato di danneggiamento, quello di danneggiamento di sistemi informatici; di seguito alla violazione di domicilio, la violazione di domicilio informatico; di seguito alla fattispecie di frode, quella informatica e così via. Una scelta differente è stata operata in Francia dove è stata creata una sezione del codice penale dedicata esclusivamente ai crimini informatici. Alcune altre fattispecie di reato sono state inserite in altri testi normativi.

Nella disamina delle fattispecie di reato, non sarà sempre indicata la misura edittale (ossia stabilita dall'atto normativo ufficiale) della pena, perché in questa sede non si ritiene utile appesantire il testo ed è invece interessante focalizzare l'attenzione sulla condotta antigiuridica.

Le prime fattispecie di reati informatici che analizzeremo sono previste nella legge n. 633 del 1941, che si occupa di protezione del diritto d'autore, così come novellata dal d.lgs. n. 518 del 1992.

All'art. 171-*bis* sono previste tre fattispecie di reato punite con la reclusione e con la multa:

1. nei casi di duplicazione (…) abusiva di programmi per elaboratori protetti al fine di trarne profitto[5];

[4] Si pensi alla responsabilità, ex art. 590 c.p., per le lesioni riportate da un soggetto derivanti dal morso di un cane lasciato libero per negligenza dal suo proprietario in un parco pubblico.

[5] È interessante notare che la nozione di 'profitto' è stata sostituita all'espressione (previgente) 'fini di lucro' per rendere più efficace e più ampia la fattispecie di reato con riguardo alla lotta alla pirateria informatica. Infatti, mentre con il termine lucro si intende un vantaggio o qualsiasi altra utilità economica quantificabile e quindi anche il risparmio di spesa, purché tale spesa sia inserita in un'attività professionale produttiva, rispetto alla quale spese ed entrate si fronteggiano almeno idealmente e danno luogo ad un saldo, invece, il significato di 'profitto' può implicare sia il lucro, quindi l'accrescimento effettivo della sfera patrimoniale, sia la mancata perdita patrimoniale ossia il depauperamento dei beni di un soggetto, del tutto sganciata da un'attività imprenditoriale.

2. nei casi di predisposizione o utilizzo di qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma;
3. nei casi di riproduzione (…), su supporti non contrassegnati SIAE, del contenuto di una banca di dati al fine di trarne profitto.

Al primo punto, dunque, è previsto che anche la creazione di una copia di un software commerciale al fine di essere donata un amico viola l'ordinamento giuridico penale.

Al secondo punto si deve notare l'anticipazione della soglia di punibilità della fattispecie riportata. Infatti, è punita la semplice condotta diretta alla rimozione o l'elusione dei sistemi di protezione dei software, che può anche prescindere dalla effettiva creazione della copia. Inoltre, il legislatore nella previsione normativa, per far sì che essa rimanga efficace, non descrive la fattispecie di reato con sufficiente determinatezza quando utilizza l'espressione 'qualsiasi mezzo'. In realtà, egli volutamente ha lasciato imprecisata la disposizione perché se avesse indicato una o più modalità specifiche sarebbero potute sfuggire dalla previsione del reato altre modalità differenti, ma aventi lo stesso scopo, e la disposizione sarebbe rimasta in molte circostanze inapplicabile e quindi inefficace.

Al terzo punto viene indicata la fattispecie di reato a protezione delle banche dati, indipendentemente dal fatto che si tratti di prodotti aventi carattere creativo o meno.

Passando alle fattispecie di reato inserite nel codice penale, si segnala la disposizione contenuta all'art. 635-*bis*, rubricata '*Danneggiamento di informazioni, dati e programmi informatici*'. La norma prevede che "Chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione …". La disposizione è posta a tutela dei beni informatici e configura un reato di danno rivolto a chi lo commette con dolo, cioè agendo consapevolmente con l'intenzione di distruggere, deteriorare, cancellare, alterare o sopprimere i detti beni ottiene il suo scopo. Il reato è perseguibile soltanto in presenza della querela della persona offesa. Allo stesso articolo, con una novella del 2016, è stata aggiunta una nuova fattispecie di reato punita con maggiore rigore quando il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore di sistema. La ragione di tale ultima circostanza aggravante è da rinvenire nella condotta del soggetto agente (l'operatore di sistema) che tradisce, per così dire, chi ha riposto fiducia in lui, oltre che nella facilità di commissione del reato essendo nelle condizioni di poter attentare al bene protetto in condizione di privilegio. Tali modalità di commissione del reato sono ulteriormente scoraggiate dalla minaccia di una pena più elevata.

L'art. 635-*ter* c.p., rubricato 'Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità', dispone che "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". Il reato è di pericolo proprio per la locuzione "fatto diretto a"; il motivo è anticipare la soglia di protezione per il bene che appartiene alla collettività e prevede l'aggravante del danno.

L'art. 635-*quater* c.p., rubricato, 'Danneggiamento di sistemi informatici o telematici', punisce con la reclusione "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 …". Anche in questa fattispecie la qualifica del soggetto agente di amministratore di sistema costituisce circostanza aggravante. Nella fattispecie il bene protetto è il sistema informatico nel suo complesso e non i dati e le informazioni.

Nel codice sono previste alcune fattispecie di reato a tutela della persona e, in particolare, nella sezione denominata 'Dei delitti contro la inviolabilità del domicilio' si trovano le disposizioni a tutela del domicilio informatico. Il domicilio informatico è inteso quale proiezione o trasposizione virtuale del domicilio fisico; è il luogo dove si esplica la personalità del soggetto, dove è riposta parte della memoria con i documenti, i pensieri personali, le fotografie, i video, le registrazioni vocali, dove si svolgono conversazioni, dove si trascorre parte sempre più cospicua del proprio tempo. In una stessa macchina possono risiedere più luoghi e quindi domicili diversi: si pensi ai profili degli utenti, distinti tramite chiavi logiche, che permettono accessi diversificati ad applicazioni, cartelle, *files*, ecc.

L'art. 615-*ter* c.p., rubricato 'Accesso abusivo ad un sistema informatico o telematico', prevede che "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 …". Da notare che è punita la condotta descritta solo quando si viola un sistema protetto, quindi, allorché si eluda un sistema di protezione oppure si rimane dentro il sistema protetto abusando della possibilità lecita, solo in un primo momento, di avervi avuto accesso. La consumazione del reato si realizza con l'ingresso nel sistema protetto, quindi il reato è di danno.

L'art. 615-*quater* c.p., rubricato 'Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici', dispone che "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 e con la multa". In questa seconda fattispecie dedicata alla violazione del domicilio informatico, il reato si perfeziona con la sola messa in pericolo del bene protetto ("mezzi idonei all'accesso"). Le pene si aggravano: 1) se l'agente è un soggetto pubblico o un investigatore o abusi di tale qualità o quella di operatore di sistema; 2) se il soggetto agente usi violenza; 3) se l'ingresso o il tentativo cagioni conseguenze dannose; 4) se si tratti di sistema di interesse pubblico.

L'art. 615-*quinquies* c.p., rubricato 'Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico', punisce con la reclusione e con la multa "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 il caso dei virus informatici intesi in forma ampia. Da notare in tale fattispecie che il soggetto agente è punibile solo se viene accertato che abbia agito con dolo e, si noti, che la soglia di punibilità è anticipata, solo per gli effetti potenziali che il virus può causare, dato che il reato si perfeziona con la messa in pericolo del bene protetto.

Il codice penale si occupa anche di reati cosiddetti di *social engineering*. Semplificando il concetto, dallo studio dei comportamenti individuali – non solo riferiti ai rapporti con gli strumenti informatici – si è ricavato che le persone hanno una propensione a rispondere a domande dirette e impreviste o ad aiutare qualcuno che sembra in difficoltà. Tali comportamenti, se vogliamo umani e solidali, sono oggetto di attenzione anche da parte dei criminali con lo scopo di sviluppare tecniche di commissione di reati tramite la persuasione psicologica per ottenere disponibilità di diverso genere, che nel mondo digitale possono consistere in denaro, in dati personali, in *password*, in informazioni riservate. Si tratta di truffe e, a livello informatico, il più delle volte la tecnica di commissione del reato consiste nell'invio di messaggi immediati o di posta elettronica del tutto simili a quelli provenienti da amministrazioni/enti/imprese/conoscenti reali e apparentemente affidabili per carpire informazioni riservate. La truffa è la fattispecie di reato – tra quelli a tutela del

patrimonio – che si occupa di punire questo genere di comportamento ed è prevista all'art. 640 c.p. Il codice si occupa anche della differente fattispecie della 'Frode informatica' prevista all'art. del 640-*ter*, nella quale è disposto che "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 e con la multa". Il reato descritto si pone in rapporto di specialità rispetto alla fattispecie della più grave truffa prevista all'art. 640 c.p. e, a differenza di quest'ultima, non sono richiesti gli artifizi e i raggiri, sostituiti nella previsione dell'art. 640-*ter* dalla manipolazione o alterazione di un sistema informatico o telematico. Anche in questa fattispecie le espressioni 'in qualsiasi modo' e 'con qualsiasi modalità' determinano un'insufficiente determinatezza della disposizione, ma sarebbe stato assai complesso, e per certi versi controproducente, per il legislatore individuare puntualmente tutte le modalità di alterazione dei sistemi informatici e telematici. Il rischio che si corre ad essere eccessivamente precisi nel descrivere le tecniche informatiche è quello di dover aggiornare con frequenza assidua la disposizione vista la rapidità dell'evoluzione tecnologica.

Tra i delitti conto la fede pubblica troviamo l'art. 491-*bis* c.p., rubricato 'Documenti informatici' nel quale è disposto che "Se alcuna delle falsità … (in atti) riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni (reclusione) … concernenti gli atti pubblici". Il regime sanzionatorio è equiparato a quello delle scritture cartacee tradizionali. È dunque sanzionata tanto la falsità materiale quanto la falsità ideologica. La prima si realizza con la contraffazione o alterazione del documento, la seconda si realizza quando si riportano dichiarazioni mendaci (dichiarazioni non veritiere).

Altre disposizioni sono dettate per garantire l'affidabilità delle firme elettroniche in senso ampio.

L'art. 495-*bis* c.p., rubricato 'Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri', dispone che "Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione".

L'art. 640-*quinquies* c.p., rubricato 'Frode informatica del soggetto che presta servizi di certificazione di firma elettronica', dispone che "Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione e con la multa".

Nel codice tra i 'delitti contro la persona', e più nello specifico tra le norme a tutela delle conversazioni e delle comunicazioni, il legislatore ha predisposto un articolo, il 623-*bis*, a tutela della riservatezza delle informazioni (voce, suoni, immagini, dati in generale) trasmesse a distanza in qualunque forma, quindi anche elettronica. Il diritto alla segretezza delle comunicazioni è in generale garantito dall'art. 15 della Costituzione. Altri articoli entrano più nel dettaglio, come l'art. 617-*quater* c.p., rubricato 'Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche', nel quale è disposto che "Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione". La stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni (intercettate). Si ponga attenzione al termine "fraudolentemente": esso lascia intendere che si possa intercettare legittimamente cioè non contravvenendo all'ordinamento giuridico. In effetti, in casi assolutamente eccezionali le intercettazioni sono consentite[6].

L'art. 617-*quinquies* c.p., rubricato 'Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche', prevede che "Chiunque, fuori

[6] V. *infra* quanto riportato all'art. 266 del codice di procedura penale.

dei casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni … è punito con la reclusione". Rispetto alla fattispecie precedente si noti l'anticipo della soglia d punibilità: si è puniti solo per il fatto di installare apparecchiature atte a ...

L'art. 617-*sexies* c.p., rubricato 'Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche', dispone che "Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione".

Come si anticipava poco sopra, ai sensi dell'art. 266 del codice di procedura penale, l'intercettazione di comunicazioni o conversazioni è consentita, in linea di principio, nei procedimenti relativi a: a) delitti dolosi per i quali è previsto l'ergastolo o una reclusione di oltre 5 anni; b) delitti gravi contro la PA; c) delitti concernenti sostanze stupefacenti o psicotrope; d) delitti concernenti armi o sostanze esplosive; e) contrabbando; f) delitti di usura, minaccia, abusiva attività finanziaria, …; g) pornografia minorile, *stalking*, contraffazione opere dell'ingegno, commercio di prodotti falsi.

Alcune fattispecie su cui è utile soffermarsi sono legate al grave e dilagante fenomeno della pedopornografia, trattate nella sezione dedicata ai delitti contro la libertà individuale al fine di garantire l'integrità fisica e psichica dei soggetti minori degli anni 18.

L'art. 600-*ter*, c.p., rubricato "Pornografia minorile", al terzo comma, dispone che "Chiunque, … con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde o pubblicizza il materiale pornografico…, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto è punito con la reclusione e con la multa …", specificando ai commi successivi che "Chiunque … offre o cede ad altri, anche a titolo gratuito, il materiale pornografico … la pena è aumentata … ove il materiale sia di ingente quantità" e che "Chiunque assiste a esibizioni o spettacoli pornografici in cui siano coinvolti minori di anni diciotto". Lo stesso articolo dà un'interpretazione di sé stesso chiarendo che "Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione (anche virtuale), con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali". Le attività di contrasto approntate dal Governo sono diverse, ricordiamo principalmente l'attivazione di un centro di monitoraggio presso il Ministero dell'Interno, l'istituzione dell'obbligo per i *provider* di segnalare siti a rischio e di filtrarli, i blocchi dei pagamenti tramite moneta elettronica e l'utilizzo del cosiddetto 'agente provocatore' o 'agente sotto copertura', cioè un agente che si finge vittima per cogliere in flagranza di reato l'adescatore criminale.

L'art. 600-*quater* c.p., rubricato "Detenzione di materiale pornografico", prevede la pena della reclusione e della multa per "Chiunque … consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto", prevedendo un aumento di pena laddove il materiale detenuto sia di ingente quantità.

Infine, un cenno va fatto alla recente previsione normativa (del luglio 2019) per contrastare il diffusissimo fenomeno del "revenge porn". Il codice penale detta la relativa disciplina all'art. 612-*ter*, rubricato "Diffusione illecita di immagini o video sessualmente espliciti". Il testo dell'articolo è il seguente, "… 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 reclusione … e con la multa …". Sempre più spesso le immagini, i video e le registrazioni audio (stranamente non ricomprese nel testo normativo) che vengono realizzati con gli strumenti informatici, più o meno tascabili, contengono aspetti personali altrui che possono essere utilizzati in maniera impropria. Non si contano, in ogni strato culturale, le violazioni della riservatezza e sono assai diffuse le pratiche di violenza psicologica derivanti da ricatti e minacce ai danni dei soggetti registrati. Questi, non sempre

consapevoli di essere "finiti" nelle memorie altrui, possono subire le pressioni psicologiche di ogni genere da parte di chi sfrutta quei contenuti per ottenere vantaggi economici e non o, semplicemente, per vendetta. Al secondo comma è previsto che "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. Qui, la previsione tende a contrastare la facile gogna mediatica che un soggetto può subire in un attimo con il propagarsi a dismisura dei contenuti privati con i sistemi social. L'articolo segue prevedendo alcune circostanze aggravanti del reato e, al terzo comma, prevede un aumento di pena "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. Da ultimo, è prevista una pena aumentata anche "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".

Per aumentare le attività di contrasto al fenomeno dei crimini informatici, nel 2004, è stata istituita l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), la cui attività di monitoraggio, di consulenza alle istituzioni e di contrasto al *cybercrime* se oggi risulta indiscutibilmente utile, per il prossimo futuro andrebbe quantomeno potenziata.

Con prevalente funzione di analisi del fenomeno del crimini informatici in Italia vi è l'Associazione italiana per la sicurezza informatica, che redige annualmente l'interessante rapporto CLUSIT nel quale fornisce un'interpretazione neutra e ragionata dell'evoluzione delle minacce cibernetiche nel panorama nazionale ed internazionale.