**UNIVERSITÀ DEGLI STUDI DI GENOVA**

**SCUOLA DI SCIENZE SOCIALI**

**DIPARTIMENTO DI GIURISPRUDENZA**

CORSO DI LAUREA IN DIRITTO PENALE

*Tesi di laurea in Diritto penale*

# "I REATI INFORMATICI COME MECCANISMO DI AGGRESSIONE ALLA PERSONA E AL PATRIMONIO"

Relatore:
*Chiar.mo Prof. Federico Consulich*

Candidato:
*Giorgia Puppo*

Anno accademico 2022-2023

# INDICE

## CAPITOLO I

## I REATI INFORMATICI E LA GENESI NORMATIVA



## CAPITOLO II

## LE FRODI *ONLINE*: IL REATO DI FRODE INFORMATICA (ART. 640 *TER* C.P.) E IL *PHISHING*

# CAPITOLO III

## REATI INFORMATICI CONTRO LA PERSONA: LA PORNOGRAFIA VIRTUALE E IL *REVENGE PORN*

# CAPITOLO I

# I REATI INFORMATICI E LA GENESI NORMATIVA

SOMMARIO: 1. La controversa definizione di "reato informatico". -2. La lotta alla criminalità informatica a livello sovranazionale e nazionale. -2.1. La Raccomandazione del Consiglio d'Europa n. 9 del 1989- 2.2. La Legge n. 547/ 1993 e le sue problematiche. - 2.2.1. I problemi metodologici e le tecniche di formulazione. - 2.3. Convenzione di Budapest del 2001. - 2.4. La Legge n. 48/ 2008 di ratifica ed esecuzione della Convenzione "*Cybercrime*".

## 1. La controversa definizione di "reato informatico".

L'esplosione di *Internet* e lo sviluppo di nuove tecnologie ha reso fertile il terreno non solo per un progresso di tipo economico, di gestione del tempo e sociale, ma, e soprattutto, per nuovi tipi di comportamenti penalmente rilevanti, che hanno portato allo sviluppo di nuove pratiche criminose. Una delle conseguenze del progresso informatico è stata l'introduzione di nuovi concetti come, ad esempio, i "dati informatici"[1] che si riferiscono a una realtà nuova e diversa, anche detta "*cyberspace*"[2]. In realtà, si può osservare come non si debba parlare di realtà "diversa" rispetto a quella reale, perché infatti, l'estensione di *Internet* ha riguardato ogni aspetto della vita del singolo individuo e della collettività, comportando una sovrapposizione con la realtà "virtuale". Risulta essere quindi più opportuno parlare di "spazio pluridimensionale e dinamica globale"[3], uno spazio del tutto reale che ha coinvolto tutti gli attori sociali ed economici dal settore dell'informazione a quello dei rapporti più intimi.

Questo crescente sviluppo delle reti informatiche ha determinato l'emersione di un non indifferente novero di illeciti configurabili sulla rete che prende il nome di "*Cyber crime*"[4].

---

[1] Definiti dalla Convenzione del Consiglio d'Europa sul *Cybercrime* del 2001, all'art 1 lett. b), come "qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione".

[2] L'autore FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Dir. pen. cont*, 2010, p. 2 definisce tale fenomeno come «Spazio virtuale in cui si consente la detemporalizzazione delle attività, che possono essere pianificate e svolte attraverso operazioni automatizzate programmate dall'utente, senza che vi sia la necessità della presenza fisica umana davanti allo schermo del computer».

[3] Si veda, a riguardo, PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in *Cybercrime. Diritto e procedura penale dell'informatica*, a cura di CADOPPI- CANESTRARI- MANNA- PAPA, Torino, 2019, p. 46.

[4] Termine coniato da BRENNER, *Cybercrime, cyberterrorism and cyberwarfare,* in *Revue internat. droit pénal*, 2006, fasc. 3, vol. 77, p. 453.

Secondo una definizione a tecnica, questo termine comprenderebbe l'intera classe di fattispecie criminose realizzate mediante l'utilizzo di un *computer* e si tratterebbe quindi semplicemente di crimini comuni che si presentano in una veste diversa[5].

Inizialmente, da parte della dottrina nordamericana, questo fenomeno di emersione di nuove forme di abuso degli elaboratori elettronici veniva definito come "*computer crimes*", espressione alla quale è stata affiancata quella di "*computer-related crime*" per evidenziare il fatto che nella commissione del reato il *computer* costituirebbe il mezzo utilizzato dall'autore e non l'autore[6].

A prescindere da quale termine venga utilizzato, il dubbio che ha caratterizzato gli anni successivi alla comparsa della criminalità informatica è stato quello di stabilire quali fossero gli elementi caratterizzanti queste pratiche criminose, che avrebbero non solo giustificato la creazione di una nuova categoria di reati, ma avrebbero poi consentito all'operatore del diritto una qualificazione giuridica del fatto corretta, stabilendo l'appartenenza a quella categoria. Le opinioni espresse durante lo studio della criminalità informatica, svoltasi all'interno dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) nei primi anni Ottanta, sono state le più svariate, motivo per cui, infine, si è rinunciato a dare una definizione internazionale del fenomeno. In particolare, la commissione di esperti aveva inizialmente optato per un approccio selettivo volto a elaborare una lista di atti con la funzione di indicare un minimo comune denominatore per le previsioni legislative che poi sarebbero state adottate dai Paesi[7]. La stessa commissione aveva poi constatato non solo l'impossibilità di arrivare a una definizione che potesse essere accettata da tutti gli Stati, ma soprattutto l'inutilità di questa qualora fosse stata troppo generica[8]. Infatti, dati gli aspetti complessi e singolari che caratterizzano questo fenomeno risulta impossibile darne una definizione giuridica[9].

In dottrina, nel campo criminologico, si sono susseguite diverse proposte di definizione di "*Computer crime*".

Primo tra tutti, merita di essere menzionato Tiedemann, il quale parla di "delitto nel campo dell'informatica" come categoria che ricomprende quegli atti illeciti compiuti

[5] A riguardo, l'Autrice BRENNER, in *op. cit*., p. 455 utilizza la metafora "*Old wine in new bottles*" proprio per indicare il fatto che la maggior parte dei crimini informatici si risolvono in fattispecie criminose già esistenti, ma con la sola differenza che in questo caso la condotta si caratterizza per il fatto essere realizzata a mezzo di un computer. A titolo esemplificativo, l'Autrice si serve del reato di "*fraud*" (frode).
[6] In tal senso si veda, PARKER, *Computer related crime*, in *Journal of Forensic sciences*, 1974, p. 292.
[7] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010, p. 56.
[8] PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 2.
[9] Nello stesso senso, FLOR, *op. cit*, p. 3.

mediante l'utilizzo del computer oppure in cui quest'ultimo rappresenta l'oggetto dell'azione illecita[10]. Tuttavia, questa ricostruzione non avrebbe impedito la riconduzione alla categoria di quelle fattispecie che, pur costituendo un'aggressione al bene materiale "*computer*", non differiscono da analoghe condotte già disciplinate, ma rivolte a beni giuridici differenti[11]. L'Autore ritiene inoltre che di "delitto d'informatica" si debba dare una definizione puntuale, affermando che esso consiste in "qualsiasi delitto contro i beni collegati al trattamento automatico dei dati"[12].

Parker, invece, parla di "*computer abuse*" cercando di ricomprendervi anche illeciti non necessariamente di natura penale, ma pur sempre collegati all'informatica, dai quali la l'autore ne ha ricavato un profitto e la vittima una perdita[13]. Inoltre, sempre secondo Parker, la proprietà comune tra queste fattispecie sarebbe la "conoscenza della tecnologia informatica" imprescindibile per realizzare l'azione illegale. L'Autore fa riferimento a conoscenze che risultano necessarie solo nel momento in cui venga utilizzato un sistema informatico, motivo per il quale si riconduce ad esse la caratterizzazione del fenomeno. Tuttavia, questa ricostruzione non si è dimostrata convincente, soprattutto considerata la sua capacità di ricondurre nella categoria dei reati informatici anche quegli illeciti il cui legame con un *computer* risulti del tutto casuale[14].

Secondo altri ancora, bisognerebbe adottare un approccio in concreto, facendo dipendere la qualificazione di un illecito come informatico dal fatto che questo non si sarebbe verificato negli stessi termini e con la stessa intensità se non fosse stato usato un *computer*[15].

Lo sviluppo continuo di queste nuove forme di criminalità ha reso difficile l'impresa di giungere a una definizione unica ed esatta.

Secondo Sarzana, si può parlare di una categoria generale di "*computer crimes*" che ricomprende tutti quegli illeciti aventi ad oggetto il *computer* o quelli in cui quest'ultimo costituisce mezzo materiale o simbolico[16].

---

[10] Come spiegato da SARZANA DI S. IPPOLITO, *in Criminalità e tecnologia: il caso dei computer- crimes*, in *Rass. penit. Criminol*., 1979, fasc. 1- 2, p. 58, si deve trattare di un delitto in cui l'influenza sul funzionamento di un computer costituiscono lo scopo oppure lo strumento dell'azione.

[11] PECORELLA, *op. cit*, p. 4 utilizza come esempio il caso in cui venga danneggiato il *monitor* di un computer o avvenga il furto di quest'ultimo. Questi sono tutti casi in cui la condotta non si distingue da quella prevista nell'ambito di una fattispecie di reato tradizionale già disciplinata.

[12] Definizione riportata da SARZANA DI S. IPPOLITO, in *Criminalità e tecnologia, cit*., p. 59, la quale richiama a riguardo TIEDEMANN, *Phénoménologie des infractions économiques*, in *Aspects criminologiques de la délinquance d'affaires*, Strasburg, 1978, p. 231.

[13] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto pena*le, cit., p. 57.

[14] PECORELLA, *op.cit*., p. 6.

[15] SARZANA DI S. IPPOLITO, in *Criminalità e tecnologia*, cit., p. 59.

[16] *Ibidem,* per mezzo simbolico si intende il caso in cui la convinzione di infallibilità dei dati del computer venga utilizzata dall'autore per la commissione dell'illecito al fine di trarre in inganno la vittima.

In base a una dottrina nordamericana[17], nell'ambito della categoria generale sono presenti tre sub divisioni: crimini in cui il sistema informatico rappresenta lo strumento mediante il quale si cerca di ricavare un profitto; crimini in cui l'obbiettivo dell'attività criminale consiste nel danneggiare il *computer* o il sistema informatico; crimini in cui il *computer* rappresenta un elemento della condotta, ma non necessariamente lo strumento o l'obbiettivo di quest'ultima[18].

Facendo, invece, una distinzione dal punto di vista del diritto sostanziale, la generale categoria dei reati informatici può essere suddivisa in due gruppi: i reati informatici in senso stretto e i reati informatici in senso lato[19].

Nella prima categoria rientrano quelle fattispecie caratterizzate da elementi tipizzanti[20] in cui il sistema informatico o il *computer* costituiscono elemento imprescindibile per la commissione del fatto[21]. Infatti, l'elemento che caratterizza questa categoria di reati consiste proprio nella "connessione in rete e fruibilità del *cyberspace*"[22], come, ad esempio, la frode informatica *ex* articolo 640 *ter* c.p. o l'accesso abusivo a sistemi informatici *ex* articolo 615 *ter* c.p.[23]. In questi casi, si può notare come l'elaboratore informatico o il sistema informatico costituiscano lo strumento utilizzato per la commissione del fatto illecito, oppure l'oggetto passivo su cui la condotta esplica i suoi effetti negativi[24].

---

[17] Vedi BRENNER, *Cybercrime Metrics: Old Wine, New Bottles*, in *Virginia JL & Tech*, 2004, vol. 9, n. 13, p. 4- 6 in cui l'Autrice si chiede se il fenomeno della criminalità informatica si risolva in fattispecie già esistenti, ma che si presentano in una veste nuova, ovvero di nuovi crimini.

[18] Ricostruzione prospettata da SARZANA DI S. IPPOLITO, in *Criminalità e tecnologia,* cit., p. 59; ID., in *Informatica, internet e diritto penale*, cit., p. 63. Analogamente FLOR, *op. cit*, p. 5 e MATTARELLA, *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Dir. pen. proc*., fasc. 6, 2022, p. 810.

[19] FUMO, *La condotta nei reati informatici*, in *Arch. Pen*., 2013, fasc. 3, p. 777.

[20] Intesi da FLOR, *op. cit*, p. 4 come elementi connessi a procedimenti di automatizzazione di dati o informazioni, ovvero legate a modalità, oggetti o attività di carattere tecnologico.

[21] AMATO MANGIAMELI- SARACENI, *Reati informatici: elementi di teoria generale e principali figure criminose*, Torino, 2015, p. XIII.

[22] FLOR*, op. cit*, p. 5.

[23] LUBERTO, *I reati informatici contro il diritto alla privacy. La tutela fornita dal d. lg n. 196 del 2003 e dal Codice penale*, in Giur. Mer., fasc. 3, 2008, p. 2 secondo il quale le fonti normative dei reati informatici in senso stretto sono, nel nostro ordinamento: la l. n. 547 del 1993 (il primo intervento organico del legislatore in materia), che ha inserito nel corpo del codice penale numerose figure di crimini informatici; la l. n. 269 del 1998, che ha introdotto l'art. 600 ter c.p. (il quale sanziona, al comma 3, anche la pornografia minorile telematica); l'art. 12 d.l. 13 maggio 1991, n. 143 (che punisce l'abuso di carte di credito, di pagamento e di documenti che abilitano al prelievo di denaro contante); la l. n. 633 del 1941 (c.d. legge sul diritto d'autore), che agli artt. 171 e seguenti prevede anche violazioni informatiche del diritto d'autore; l'art. 6 d.lg. 15 novembre 2000, n. 373 (tutela delle trasmissioni ad accesso condizionato); il d.lg. n. 196 del 2003 (c.d. Codice della privacy), il quale, negli artt. da 167 a 171 contempla figure di reato a tutela della riservatezza dei dati personali e dell'azione del Garante della Privacy.

[24] Esempi utilizzati da PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee, in Riv. trim. dir. pen. ec.,* 2011, fasc. 4, p. 827.

La seconda categoria, invece, ricomprende quelle fattispecie "comuni" che possono essere agevolmente applicate a fatti posti in essere con l'utilizzo della tecnologia. Questo sottogruppo prende anche il nome di reati "*Cibernetici*"[25]: si sta facendo riferimento a fattispecie che si sono diffuse grazie all'evoluzione tecnologica, ma che hanno come oggetto dell'aggressione dei beni preesistenti rispetto all'avvento della tecnologia[26]. Un esempio potrebbe essere la diffamazione *online,* punita ai sensi dell'articolo 595 c.p.[27]. Essa è un reato eventualmente informatico che può venire in essere anche, ma non solo, con la pubblicazione sulla rete di commenti offensivi della reputazione altrui[28]. Quindi, si sta parlando di fattispecie che possono essere concretizzate a prescindere dalla componente tecnologica, la cui eventuale esistenza rappresenta una possibile modalità di concretizzazione della condotta.

Questa suddivisione è funzionale non solo da un punto di vista classificatorio, ma anche sostanziale, ed è volta a evidenziare le differenze intercorrenti tra queste fattispecie in termini di beni giuridici e metodologie di tipizzazione diverse[29].

Sotto un punto di vista processuale, questa ricostruzione trova riscontro nelle disposizioni previste dalla Convenzione sulla criminalità informatica del Consiglio d'Europa, le quali trovano applicazione oltre che ai reati da essa stessa previsti dagli artt. 2 a 11, anche agli illeciti commessi per mezzo di sistemi informatici[30].

Non solo, infatti, un approccio simile è stato poi utilizzato dal Comitato nominato in seno al Consiglio d'Europa nel formulare la lista minima e facoltativa che ha costituito poi un punto di riferimento internazionale in materia di criminalità informatica[31].

---

[25] PICOTTI, *Cybercrime e diritto penale*, in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di PARODI- SELLAROLI, Milano, 2020, p. 712, secondo il quale, affianco ai reati in senso stretto, i quali includono fra i loro elementi costitutivi, elementi tecnico- informatici, è emersa la categoria dei reati cibernetici, o anche detti reati in senso lato, che pur non presentando le sopradette caratteristiche tecnico-informatiche, meritano rilievo giuridico e processuale data la necessità di contrastarli con adeguate sanzioni e specifici strumenti di tutela se commessi in rete.

[26] AMATO MANGIAMELI- SARACENI*, op. cit.,* p. XIII.

[27] Esempio utilizzato da LUBERTO, *op. cit*, p. 1- 2.

[28] PIETRELLA, *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle Botnets*, in *disCrimen*, 2021, p. 4.

[29] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale,* cit., p. 59.

[30] La Convenzione Cybercrime di Budapest del 2001, nel delineare all'art 14, par. 2, il campo di applicazione della Sezione II, in materia di diritto processuale, include alla lettera b) qualsiasi reato commesso tramite sistemi informatici. Concorde MATTARELLA, *op. cit.,* p. 810.

[31] PECORELLA, *op. cit*, p. 7. Analogamente PICOTTI, *op.cit.,* p. 712, in cui si legge che la lista minima inserita nella Raccomandazione del 1989 sulla "criminalità informatica", contenente otto incriminazioni, fa riferimento ai reati informatici in senso stretto.

## 2. La lotta alla criminalità informatica a livello sovranazionale e nazionale.

La portata del fenomeno della criminalità informatica è stata notevole, tanto da richiedere un tempestivo intervento a livello internazionale per predisporre politiche di contrasto ai reati commessi sulla rete e nella rete. È un fenomeno con un potenziale criminoso molto elevato che ha portato non solo all'emersione di fattispecie nuove, ma ha reso più agevole e subdola la commissione di quelle fattispecie già presenti nella realtà comune inserendo una nuova possibile modalità di condotta.

Partendo da questo assunto, è agevole pensare come il tema sia stato trattato e discusso in varie sedi, come l'Organizzazione per la Cooperazione e lo Sviluppo Economico e il Consiglio d'Europa, cercando di arrivare all'adozione di politiche confacenti alle esigenze di tutti i paesi, ma anche da un punto di vista più specifico proponendo manovre mirate e dirette alla gestione di una determinata problematica. Un esempio è stata la Direttiva 2011/93/UE sulla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile o ancora la proposta di Direttiva del Parlamento europeo e del Consiglio sugli attacchi contro i sistemi di informazione.

A dimostrazione di quanto il tema della criminalità informatica sia sentito non solo a livello nazionale ma anche sovranazionale, si annovera il fatto che sia stata inserita nel Trattato di Lisbona, all'articolo 83, come fenomeno di una certa gravità e di natura transazionale su cui l'Unione Europea esercita una competenza di tipo penale[32].

Inoltre, un fondamentale contributo alla diffusione di una tipologia unitaria di *computer crimes* è stato dato da un rapporto elaborato dal Comitato europeo in cui sono stati distinti in modo dettagliato i vari tipi di abuso, attribuendo a ciascuno una definizione[33].

### 2.1. La Raccomandazione del Consiglio d'Europa n. 9 del 1989.

Nel 1985, il Consiglio d'Europa nominò un Comitato ristretto di esperti, il Comitato dei Ministri del Consiglio d'Europa, preposto all'analisi del fenomeno della criminalità informatica e alla predisposizione di regole e dei principi funzionali alla legislazione nazionale dei vari Paesi. Il rapporto che venne stilato fu poi inserito integralmente e costituì

[32] FLOR, *op. cit.*, p. 2
[33] CONSEIL DE L'EUROPE, *La criminalité informatique: recommandation n° r (89) 9 sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels*, Strasburg, 1990.

la base della Raccomandazione n. 9 del 1989 "*sur la criminalitè en relation avec l'ordinateur*" adottata il tredici settembre[34].

In essa non si rinviene una definizione di "criminalità informatica", ma ci si riferisce a quest'ultima come una "nuova sfida", sottolineando il suo carattere transfrontaliero[35], riconoscendo quindi la necessità di un intervento immediato e adeguato a questa nuova situazione[36].

Questo fenomeno iniziò a suscitare l'interesse[37] anche di enti di ricerca costituiti specificatamente per l'analisi della vulnerabilità dei sistemi informatici in Europa e l'impatto derivante dagli accessi abusivi e frodi informatiche. Un esempio è la ricerca che venne svolta nel 1983 dall'Istituto per le Studio della Vulnerabilità delle Società Tecnologicamente Evolute (ISTEV, ora abolito) da cui emersero ben tredici attacchi ad aziende italiane tra il 1970 e 1983. Questi risultati furono utili non solo a rivelare la scarsa propensione delle aziende a denunciare questi crimini, ma anche a dimostrare la dimensione del fenomeno della criminalità informatica[38] e le carenze con riguardo agli strumenti di tutela che avrebbero comportato un aumento dei rischi di danni economici, anche di gravi entità, derivanti da questi crimini informatici.

Il Comitato dovette affrontare due ostacoli diversi. Il primo consisteva nel tenere in considerazione l'elemento di prevenzione generale che avrebbe dovuto caratterizzare l'intervento penale, così da anticipare l'eventuale crescita di questa tipologia di crimini. Il secondo consisteva invece nel fare i conti con l'inadeguatezza delle misure già presenti nel diritto penale dei singoli Stati e con il principio di legalità[39].

Il lavoro del Comitato incaricato dal Consiglio in materia di criminalità informatica si concluse nel 1988 con l'elaborazione di due liste di diverse condotte abusive, una "minima", o "minimale"[40], e una "facoltativa".

Nella prima furono inserite le fattispecie considerate necessarie che, secondo l'opinione unanime del Comitato, tutti gli Stati erano chiamati a perseguire e sanzionare con la pena

---

[34] PECORELLA, *op. cit*., p. 7.
[35] FROSINI, *La criminalità informatica*, *Dir. inform*., 1997, fasc. 3, p. 489.
[36] MAZZA, *Prevenzione e repressione in tema di reati informatici*, in *Oss. pen*., 2014, p. 2.
[37] MAZZA, I*bidem,* ove si afferma che le indagini degli anni'80 hanno mostrato il carattere reale della criminalità informatica sia sul piano economico che giuridico, richiedendo un'attenzione particolare da parte del legislatore per offrire senza ritardi strumenti idonei a sopperire alla vulnerabilità dei sistemi informatici.
[38] BLENGINO, *I reati della rete e la costruzione dei rischi nello spazio digitale*, in *Antigone Quadrimestrale di critica del sistema penale e penitenziario*, n. 3, 2008, p. 108- 109.
[39] MAZZA, *op. cit*, p. 2.
[40] FROSINI, *op. cit.*, p. 489. A detta dell'Autore questa lista ricomprendeva quelle figure illecite per le quali appariva urgente e necessario provvedere a una serie di sanzioni giuridiche, in quanto reati già conosciuti e diffusi.

ovvero interventi *ad hoc*[41]. I comportamenti inclusi in questa lista rientravano nelle seguenti tipologie:

La *frode informatica* intesa quale "ingresso, alterazione, cancellazione o soppressione di dati o programmi informatici, o qualsiasi altra ingerenza in un trattamento informatico che ne influenzi il risultato, e che determini per ciò stesso un pregiudizio economico o materiale ad un'altra persona, effettuato con l'intento di ottenere un vantaggio economico illegittimo per se stesso o per altri"; *falso in documenti informatici* come "ingresso, alterazione, cancellazione o soppressione di dati o programmi informatici o qualsiasi altra ingerenza nel trattamento informatico, effettuate con modalità o condizioni tali da costituire, secondo il diritto nazionale, un reato di falso qualora i fatti stessi fossero commessi nei riguardi di uno degli oggetti tradizionali di questo tipo di infrazione"; *danneggiamento di dati o programmi informatici* come "cancellazione, danneggiamento, deterioramento o soppressione senza diritto di dati o programmi informatici"; *sabotaggio informatico* come "ingresso, alterazione, cancellazione o soppressione di dati o programmi informatici ovvero ingerenza nei sistemi informatici, con l'intenzione di ostacolare il funzionamento di un sistema informatico o di un sistema di telecomunicazione"; *accesso non autorizzato* inteso come "accesso senza diritto ad un sistema o ad una rete informatica mediante violazione delle regole di sicurezza"; *intercettazione non autorizzata* intesa come "attuata senza diritto e mediante mezzi tecnici di comunicazioni inviate, provenienti o esistenti nell'interno di un sistema o di una rete informatica"; *riproduzione non autorizzata di un programma informatico protetto* come "riproduzione, diffusione o comunicazione al pubblico, senza diritto, di un programma informatico protetto dalla legge"; *riproduzione non autorizzata di una topografia* intesa come "riproduzione senza diritto di una topografia, protetta dalla legge, di un prodotto a semiconduttori, o sfruttamento commerciale ovvero importazione a tale scopo, senza averne diritto, di una topografia o di un prodotto semi- conduttore fabbricato con l'aiuto di tale topografia"[42].

Nella lista facoltativa furono inserite invece quelle fattispecie per le quali non si era ancora raggiunto un giudizio unanime circa come perseguirle, lasciando quindi la valutazione alla discrezionalità di ciascuno Stato[43]. In questa rientravano:

*L'alterazione di dati o di programmi informatici non autorizzati*; *spionaggio informatico* ossia "l'ottenimento, mediante mezzi illegittimi, quali la divulgazione non autorizzata, il trasferimento o utilizzazione senza diritto né altra giustificazione legale, di un segreto commerciale o industriale, con l'intenzione di causare un pregiudizio economico all'avente diritto al segreto o di ottenere per se stesso o per altri un vantaggio economico illecito"; *utilizzazione non autorizzata di un elaboratore* che consiste "nell'utilizzazione senza diritto di un sistema o di una rete informatica effettuata accettando un rischio rilevante di causare un pregiudizio a colui che ha diritto di utilizzare il sistema o di arrecare pregiudizio al sistema o al suo funzionamento, ovvero con l'intenzione di creare un pregiudizio alla persona che ha diritto di utilizzare il sistema o di arrecare pregiudizio al sistema o al suo funzionamento, ovvero causando in tal modo un pregiudizio alla persona che ha diritto di utilizzare il sistema o arrecando un pregiudizio al sistema o al suo funzionamento"; *utilizzazione non autorizzata di un programma informatico protetto* cioè "l'utilizzazione senza diritto di un programma protetto dalla legge o riprodotto senza diritto, con l'intenzione di ottenere un vantaggio economico illecito per sé stesso o per altri, o di causare un pregiudizio al detentore di tale diritto"[44].

La Raccomandazione del Consiglio aveva come obbiettivo quello di portare l'attenzione dei legislatori nazionali sulla necessarietà di una politica uniforme tra i diversi Stati sia per far fronte ai rischi derivanti dai cosiddetti "paradisi informatici", che in virtù dell'importanza

[41] PECORELLA, *op. cit.*, p. 8.
[42] Elencazione riportata da PICA, *Diritto penale delle tecnologie informatiche. Computer's crimes e reati telematici internet banche dati e privacy*, Torino, 1999, p. 15.
[43] PECORELLA, *op. cit.*, p. 8.
[44] PICA, *ivi*, p. 16.

di una stretta cooperazione tra ordinamenti nella lotta contro la criminalità informatica, avendo questo carattere sovranazionale[45].

L'adesione rispetto al contenuto della Raccomandazione trova la propria conferma negli studi svolti dal XV Congresso, in seno *all'Association Internationale de Droit Pénal* (AIDP), in materia di criminalità informatica. In questa occasione, infatti, registrato il consenso degli Stati a sanzionare anche i comportamenti contenuti nella lista facoltativa, si era avanzata la proposta di unire le due liste. Inoltre, il Congresso propose un aggiornamento delle linee contenute nella Raccomandazione del Consiglio, arrivando, nel 1994, all'emissione di una Relazione finale volta a sollecitare gli Stati ad un ampliamento dei comportamenti abusivi, dovendo essere aggiunti sia il "commercio di codici di accesso illecitamente ottenuti o di altre informazioni sulla possibilità di conseguire un accesso non autorizzato a dei sistemi informatici", che la "diffusione di programmi *virus* o programmi similari"[46].

Nella stessa Relazione si propose anche la possibilità di contrastare, non solo le condotte dolose sulle cui sole il Consiglio incentrò la propria attenzione, ma anche quelle colpose o comunque quelle che costituiscono una fonte di rischio[47].

### 2.2. La Legge n. 547/ 1993 e le sue problematiche.

Con la diffusione degli strumenti informatici, e quindi l'intuizione da parte del mondo criminale di potersi avvalere dell'elaboratore informatico per realizzare condotte illecite, è venuta alla luce la questione su come si potesse contrastare questo nuovo fenomeno senza violare il principio di legalità e tassatività delle norme penali *ex* artt. 1 del Codice penale e 25, comma due, della Costituzione[48]. Soprattutto, sotto il punto di vista della casistica giudiziale, i giudici hanno riscontrato fin da subito difficoltà nel gestire e qualificare correttamente quei fatti connotati da un collegamento con l'elemento tecnologico. A titolo di esempio, una delle pronunce che fu oggetto di critica da parte della dottrina ha riguardato la riconduzione della condotta di colui che aveva manomesso il *software* di un *computer* di proprietà di un'Università, così da interromperne il funzionamento, al reato di "attentato a impianto di pubblica utilità" *ex* articolo 420 c.p. I problemi in questa ricostruzione erano

[45] PECORELLA, *op. cit*., p. 9.
[46] PECORELLA, *Ivi*, p. 10.
[47] PECORELLA, *Ivi*, p. 11.
[48] DESTITO- DEZZANI- SANTORIELLO, *Il diritto penale delle nuove tecnologie*, Milano, 2007, p. 58.

due: *in primis*, il bene che risultava aggredito non sembrava essere il "senso di sicurezza della collettività" e, *in secundis*, risultava estremamente difficoltoso ricondurre nella nozione "impianto", come intesa dalla giurisprudenza, il "sistema informatico"[49]. Ancora, con riguardo alla truffa informatica, risultava difficile il riferimento all'induzione in errore della persona offesa, in quanto era frequente che l'inganno non fosse rivolto alla persona, quanto piuttosto a un elaboratore informatico. In altri casi, invece, risultava mancare un atto di disposizione patrimoniale proveniente dalla vittima, poiché spesso il vantaggio veniva raggiunto solo grazie a un utilizzo improprio del *computer*[50]. Non sono ovviamente mancati i casi in cui si è optato per l'applicazione del reato di truffa anche a condotte poste in essere mediante elaboratore. In questi casi, ad esempio, si è sostenuto che l'inganno non avesse colpito solo il *computer* ma anche il personale preposto al suo utilizzo, ricostruendo così l'elemento costitutivo del reato di truffa[51].

Gli interpreti si trovavano, quindi, di fronte a delle lacune normative in assenza di norme *ad hoc* contro i reati informatici, peraltro non colmabili interpretativamente nel rispetto degli artt. 25 Cost. (principio di legalità e di determinatezza) e 14 Preleggi (divieto di analogia in materia penale)[52]. Ragion per cui, il legislatore italiano, dagli inizi degli anni Novanta ha dato avvio a un "diritto penale dell'informatica", comprensivo di numerose fattispecie incriminatrici caratterizzate da severi livelli sanzionatori, ma senza sistematicità[53].

Inizialmente, le esigenze di tutela sono state soddisfatte con interventi diretti a far fronte ad emergenze occasionali: un esempio è rappresentato dal Decreto-legge n. 143 del 1991, convertito in Legge il 5 luglio dello stesso anno, ove all'articolo 12 si incriminavano le frodi e gli abusi su carte di credito e bancomat[54]. Altre volte, invece, le norme sono state adottate in attuazione di Direttive e raccomandazioni di fonte sovranazionale portando a interventi

---

[49] Trib. Firenze, 27 gennaio 1986, in *Foro. it*, 1986, II, c. 359.
[50] DESTITO- DEZZANI- SANTORIELLO, *op. cit*., p. 59.
[51] Trib. Roma, 14 dicembre 1985, in *Dir. inform*., 1988, p. 487 avente ad oggetto il caso del dipendente bancario che, inserendo falsi dati nel computer, ha rappresentato falsamente che alcuni versamenti fossero avvenuti in contanti anziché assegni.
[52] LUBERTO, *I reati informatici contro il diritto alla privacy*, cit., p.2.
[53] In tal senso PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. internet*, 2005, fasc. 2, p. 189 e FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *Dir. pen. e proc*., 2009, fasc. 5, p. 640 in cui l'Autrice afferma che il diritto penale dell'informatica, fin dagli inizi, non è stato mai né del tutto comune, né tanto meno speciale, utilizzando categorie giuridiche tradizionali, portando a qualificare i reati informatici come reati caratterizzati dal mezzo di aggressione. La difficoltà nell'applicare le fattispecie comuni e il colmare delle lacune, «ha portato ad identificare un diritto penale dell'informatica che invece non è mai nato: esso, infatti, non è stato concepito in base a un'idea costitutiva, ma è stato costruito attraverso l'accorpamento di materiali diversi, senza la morfologia di un organismo corrispondente a un modello, vale a dire senza disegno unitario e senza sistematicità».
[54] Si veda PECORELLA, *L'abuso dei distributori automatici di banconote*, in *Riv. it. dir. proc. pen.,* 1990, fasc. 2, p. 573.

settoriali, in cui le disposizioni si risolvono in previsioni "sanzionatorie"[55] volte a integrare precetti e discipline extra-penali. Ne sono esempio le Direttive CE 91/250 e CE 2001/29 in materia di diritto d'autore.

Soltanto la novella legislativa n. 547 del 1993 sembra aver cercato di operare in modo sistematico, modificando il Codice penale con l'inserimento di norme il più possibile accostabili a quelle preesistenti. Tuttavia, a causa della costante evoluzione che caratterizza l'universo tecnologico e la globalizzazione, non pare possa sostenersi sia stato un lavoro soddisfacente[56]. Oltre, al Codice penale, ci sono stati poi altri due campi d'intervento di notevole importanza: la Legge n. 633 del 1941, e successive modifiche, sul diritto d'autore e il Decreto legislativo n. 196 del 2003 sul trattamento dei dati personali.

In realtà, i primi progetti di legge diretti a offrire una regolamentazione del fenomeno della criminalità informatica risalgono agli anni Ottanta[57] e solo due sono precedenti alla Raccomandazione del Consiglio d'Europa. Solo nel 1993, con l'approvazione della legge organica, recante le "Modificazioni ed integrazioni alle norme del Codice penale e del codice di procedura penale in tema di criminalità informatica", sono state consentite sia l'introduzione nel Codice penale di fattispecie di reato informatico che l'attuazione della Raccomandazione n. 9/1989 del Consiglio[58].

La Commissione fu nominata nel 1989 dall'allora Ministro Vasalli ed era composta da magistrati, accademici ed esperti informatici: nel decidere come operare, aveva optato per il modello "evolutivo"[59], ossia la predisposizione di uno schema per apportare modifiche e integrazioni alle disposizioni già esistenti nel Codice penale, così da estenderne l'applicazione.

Nello stesso anno la Commissione procedette a una serie di audizioni di grandi aziende, pubbliche e private[60], con l'obbiettivo di raccogliere dati sulle modalità concrete dei reati

---

[55] PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di internet*, a cura di PICOTTI, Padova, 2005, p. 30, parla di una categoria "aperta" che ricomprende quelle disposizioni di carattere meramente sanzionatorio delle discipline extra penali, che non stabiliscono pene o sanzioni, ma si limitano a prescrivere agli Stati membri di garantire, in sede di attuazione, l'effettività della loro applicazione, mediante sanzioni efficaci, proporzionate e dissuasive.

[56] PICOTTI, *Internet e diritto penale*, cit., p. 190.

[57] Per un approfondimento ORTU-CIFALDI, *I disegni di legge in materia di reati informatici*, in *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89) - 9 e la Legge 23 dicembre 1993 n. 547 in materia di computer crimes: un'analisi comparativa*, a cura di ELMI, in *Informatica dir*., 1996, fasc.1, p. 116.

[58] PICA, *op. cit.,* p. 19.

[59] RESTA, *Informatica, telematica e computer crimes*, in *Informatica dir*., 1997, fasc. 1, p. 145.

[60] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale,* cit., p. 184, in base al quale fu presentato un questionario a nove organizzazioni, tra cui: INPS, INAIL, IPACRI, Confindustria, ANIA, ABI, ASSOFT, ANASIM, ASSINTEL.

informatici e l'andamento di questo fenomeno. Dopo diverse perplessità e timori manifestati dai parlamentari durante i lavori, che hanno fatto emergere non solo la loro intraprendenza, ma anche la loro impreparazione e poca conoscenza del fenomeno[61], arrivò l'approvazione del Parlamento nel dicembre del 1993.

Con questa novella sono state introdotte nel Codice penale tutte le fattispecie contenute nella "lista minima" della Raccomandazione del Consiglio d'Europa del 1989 e alcune fattispecie della "lista facoltativa" come, ad esempio, l'alterazione dei dati[62]. Per quanto riguarda la collocazione topografica dei reati informatici, la maggior parte di questi è stata inserita nell'ambito del Libro II, sottolineando così l'importanza dei beni giudici tutelati in quanto primari per la collettività. Su quattordici reati, dieci di questi sono stati collocati nel Capo III (delitti contro la libertà individuale) del Titolo XII (Delitti contro la persona). In particolare: nella Sezione I, in virtù dell'oggetto della tutela, è stato inserito l'art. 600 *ter*[63], nella Sezione IV (Delitti contro la inviolabilità del domicilio) sono stati ricompresi gli articoli 615 *ter, quater e quinquies*; nella Sezione V (Delitti contro la inviolabilità dei segreti) invece, gli articoli 616, 617 *quater, quinquies, sexies*, 621 e 623 *bis*; nel Titolo XIII (Delitti contro il patrimonio), invece, sono stati collocati gli articoli 635 *bis* e 640 *ter.* Sempre nel Capo III, al Titolo III (Delitti contro l'amministrazione della giustizia) è stato inserito l'articolo 392, al Titolo V (Delitti contro l'ordine pubblico) l'articolo 420 e, infine, al Titolo VII (Delitti contro la fede pubblica) l'articolo 491 *bis*[64].

### 2.2.1. I problemi metodologici e le tecniche di formulazione.

La Commissione nominata dal ministro Vasalli ha dovuto affrontare diversi problemi nel corso della preparazione della Legge del 1993, uno dei quali rappresentato dalla scelta di modificare il Codice penale piuttosto che promuovere una legge speciale. La valutazione

[61] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale,* cit., p. 185- 186, inserisce qualche esempio a riguardo come la perplessità espressa dal relatore riguardo l'integrazione prevista per l'articolo 392 c.p. L'affermazione in base alla quale l'integrazione avrebbe comportato l'inclusione di una fattispecie già ricompresa nell'articolo e quindi si sarebbe trattato di una integrazione superflua, dimostrava come la relazione al disegno di legge non fosse stata letta con attenzione. Un altro deputato "scopriva" che l'articolo 392 c.p., anche se integrato avrebbe lasciato scoperte alcune fattispecie come colui che si introduce in un sistema senza rivendicare l'esercizio di un diritto (…), non considerando l'articolo quattro del disegno di legge e l'introduzione dell'articolo 615 ter in materia di accesso abusivo.
[62] PICOTTI, *Sistematica dei reati informatici,* cit., p. 33.
[63] PICOTTI, *Internet e diritto penale,* cit., p. 190. La novella è stata poi completata con la Legge contro la pedofilia del 1998 n. 269 che ha introdotto, oltre ad altre fattispecie, anche il delitto di diffusione di materiale pedopornografico "anche per via telematica".
[64] PICOTTI, *Sistematica dei reati informatici,* cit., p. 44.

operata dalla Commissione portò a prediligere la prima opzione. Le motivazioni[65] che spinsero i commissari verso questa direzione si basarono non solo sulla considerazione che la specialità della materia non fosse tale da giustificare la produzione di una legge *ad hoc*; essi fecero anche leva sull'identità dei beni giuridici tutelati delle nuove fattispecie e quelli oggetto di disposizioni già presenti all'interno del Codice penale[66].

In particolare, agli occhi della Commissione le figure che sarebbero state introdotte apparivano come nuove modalità volte all'aggressione di beni giuridici già tutelati nel Codice[67].

Secondo una parte della dottrina[68], non appare definitivamente individuabile un unico bene giuridico che accomuni tutte le fattispecie caratterizzate da nuove tecnologie. Risulta invece possibile individuare il singolo bene tutelato dalla singola disposizione, senza doversi allarmare qualora questo risulti già tutelato. Infatti, uno dei vantaggi derivanti dall'aver deciso di inserire le nuove fattispecie in corrispondenza delle fattispecie comuni, tenendo fermo il criterio basato sul bene giuridico offeso, è quello di poter evidenziare analogie con le preesistenti norme anche con riguardo al trattamento sanzionatorio. Questo parallelismo svolge anche la funzione di "legittimazione" delle nuove fattispecie. Tale ricostruzione appare però fuorviante[69]. Infatti, la partizione sistematica di questi reati consente di suddividere questi ultimi in tre categorie: 1) fattispecie che offendono con nuovi mezzi o modalità di aggressione beni giuridici tradizionali, esempio è la frode informatica, in cui alla tutela del tradizionale bene "patrimonio" si affianca quella della corretta e fedele attivazione ed esecuzione delle procedure automatizzate che caratterizzano il *computer*; 2) fattispecie che offendono beni tradizionali, in cui la diversità degli oggetti passivi su cui si esplicano gli effetti della condotta, si rispecchia anche sui beni tutelati: un esempio in tal senso può essere rappresentato dalle falsità informatiche *ex* art. 491 *bis* c.p.[70], ove il bene della fede pubblica viene tutelato diversamente rispetto alle tradizionali fattispecie riguardanti la fede documentale tradizionalmente intesa. In questo caso, vista la fluidità dei dati informatici che ne consente un trattamento automatizzato, si è deciso di far leva, a fini probatori, su elementi

[65] Nella Relazione di accompagnamento dello schema del disegno di legge, in *Dir. inform*., 1992, p. 624.
[66] MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Crit. dir*., 1994, fasc. 4, p. 12.
[67] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale,* cit., p. 187, il quale afferma che il criterio utilizzato dal legislatore del 1930, nell'inserire nuovi reati, si basa sull'unità dell'oggetto giuridico, inteso come interesse di categoria. Nello sesso senso FULVI, *La Convenzione Cybercrime,* cit., p. 640- 642 e FUMO, *op. cit.,* p. 773 ss.
[68] PICA, *op.cit.,* p. 36.
[69] PICOTTI, *Sistematica dei reati informatici,* cit., p. 53.
[70] Per approfondimenti, si veda PICOTTI, *Internet e diritto penale,* cit., p. 191.

tecnici come la firma elettronica o digitale per garantire la veridicità e genuinità del contenuto del documento; 3) fattispecie che offendono nuovi beni giuridici. Infatti, con l'evoluzione tecnologica sono emersi anche nuovi interessi meritevoli di tutela come, ad esempio, l'integrità e sicurezza informatica[71].

Nel formulare le nuove disposizioni, a completamento della novella del 1993, la Commissione ha fatto uso di diverse tecniche.

La prima tra tutte, volta al superamento dei limiti applicativi propri delle fattispecie preesistenti di fronte a condotte poste in essere con l'ausilio di un mezzo tecnologico, è rappresentata dall'utilizzo di clausole definitorie degli oggetti informatici. Questa tecnica è volta all'estensione della portata di determinate nozioni penalistiche o all'introduzione di nuove. Un esempio in questo senso è costituito dell'art. 392 c.p., ove si è aggiunto un terzo comma al fine di estendere la nozione di "violenza sulle cose" a comportamenti aventi ad oggetto un programma informatico arrivando a creare il nuovo concetto di "violenza tecnologica". La *ratio* di questa integrazione si rinviene, leggendo la Relazione di accompagnamento al disegno di legge, nell'esigenza di ricondurre nell'alveo dell'articolo 392 c.p. quelle fattispecie che non potevano trovare disciplina nell'ambito dell'articolo 624, comma due c.p.[72], perché inidonee sia a rientrare nel concetto di "cosa mobile" e conseguentemente ad assumere la qualità di oggetto materiale ai fini dell'applicabilità dell'art. 392 c.p.[73]. Il suddetto comma tre, tuttavia, in quanto norma definitoria, non limita i suoi effetti con riguardo al solo art. 392 c.p., ma si estende all'intero sistema in virtù della locuzione "agli effetti della legge penale"[74]. Un altro esempio ancora è l'estensione della nozione di "corrispondenza" ex art. 616 c.p. a quella "informatica o telematica"[75].

Altre volte, il legislatore ha optato per l'inserimento di nuove fattispecie incriminatrici, la cui struttura risulta ricalcata su quella di norme già vigenti. Un esempio è rappresentato dalla frode informatica ex art. 640 *ter* c.p., modellata sullo schema della truffa comune *ex* art. 640 c.p., in cui però il bene giuridico sembra essere parzialmente diverso. Infatti, ciò che

---

[71] PICOTTI, *Ivi.*, p. 61 e ss.

[72] SARZANA DI S. IPPOLITO, *Ivi.,* p. 190 in cui si legge che la Commissione, nel verificare le condotte da inserire nel codice, ritenne che alcuni comportamenti rientrassero già in disposizioni presenti nel codice, come ad esempio le ipotesi di impossessamento di materiali collegati a sistemi informatici, quindi componenti dell'hardware o software, potevano trovare disciplina nell'ambito dell'art 624 c.p. in materia di furto. Lo stesso non poteva dirsi con riguardo alle condotte di sottrazione di dati e informazioni, i quali non si sarebbero potuti ricondurre nel concetto di "cosa mobile".

[73] MANTOVANI, *op.cit.,* p. 14.

[74] MANTOVANI, *Ibidem.*

[75] Per approfondimenti MANTOVANI, *op.cit.,* p. 12; RESTA, *op.cit.,* p. 149; SARZANA DI S. IPPOLITO, *Problemi vecchi e nuovi nella lotta alla criminalità informatica*, in *Il diritto penale dell'informatica*, cit., p. 11, a cura di PICOTTI; ID., *Internet e diritto penale,* cit., p. 190.

risulta essere leso non è tanto la libertà di autodeterminazione della vittima, quanto la correttezza del sistema informatico, colpita da alterazioni abusive[76].

La novella del 1993 è intervenuta anche sul piano processuale introducendo l'art. 266 *bis* c.p.p. (rubricato "Intercettazioni di comunicazioni informatiche o telematiche"), nel Libro III del Codice di procedura penale in materia di mezzi di ricerca della prova, in base al quale, per i reati indicati all'art. 266 c.p.p. e per quelli commessi mediante l'utilizzo di tecnologie informatiche, si ammette "l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi". Un altro intervento si è risolto nell'introduzione del comma 3 *bis* all'art 268 c.p.p., così da consentire al Pubblico ministero di disporre di impianti appartenenti a privati nell'esecuzione delle operazioni di intercettazione. La modifica ha riguardato anche i commi 6, 7 e 8 dello stesso articolo, predisponendo una disciplina per la fase di acquisizione delle prove costituite da dati registrati su supporti informatici. Infine, si è integrato l'art. 25 *ter* del Decreto- legge n. 306 del 1992, convertito con modificazioni dalla Legge n. 356 del 1992, avente ad oggetto le intercettazioni preventive, inserendovi l'espressione "ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici", adeguando quindi questa forma di intercettazione anche alle nuove tecnologie che potranno essere utilizzate qualora necessarie per l'attività di prevenzione relativa ai delitti di cui all'art. 51 comma tre *bis* c.p.p.[77].

Il merito della legge 547/1993 è stato quello di dotare l'ordinamento italiano di un novero di *computer crimes*, senza però curarsi adeguatamente degli effetti che sarebbero derivati dalle integrazioni e modifiche attuate al Codice, subendo critiche anche con riguardo alla formulazione di determinate fattispecie.

### 2.3. Convenzione di Budapest del 2001.

Dopo quattro anni di lavori, il 23 novembre del 2001 fu firmata a Budapest la Convenzione sulla criminalità informatica, atto adottato dal Consiglio d'Europa come presa di coscienza del carattere sovranazionale del fenomeno della criminalità informatica e

[76] PICOTTI, *Sistematica dei reati informatici*, cit., p. 51 e ID., *Internet e diritto penale*, cit., p. 192. La frode informatica non è l'unica figura che è stata inserita *ad hoc* nel Codice, ma sono state inserite anche le figure dei delitti di intercettazione di comunicazioni informatiche o telematiche *ex* artt. 617 *quater*, 617 *quinquies*, 617 *sexies* c.p.; dell'accesso abusivo ex art. 615 ter c.p.; del danneggiamento di dati o programmi informatici *ex* art. 635 *bis* c.p.; e della pornografia minorile *ex* art. 600 *ter* c.p., in particolare il nuovo terzo comma, introdotto con la Legge del 1998 contro la pedofilia volto a punire la distribuzione, divulgazione o pubblicazione di detto materiale "anche per via telematica".
[77] RESTA, *op.cit.,* p. 192.

impegno da parte degli Stati firmatari di arrivare a dotarsi di una disciplina uniforme e unitaria in materia. La Convenzione è entrata in vigore il 1° luglio del 2004 e rappresenta uno degli strumenti centrali, se non lo strumento internazionale più efficace[78], nel quadro sovranazionale diretto alla lotta della criminalità informatica. È un atto che riflette la consapevolezza degli Stati sull'esigenza di una ben funzionante cooperazione internazionale in campo penale per ottenere un legame stretto tra Paesi e perseguire una politica comune finalizzata alla tutela della società contro un fenomeno dematerializzato e caratterizzato dall'assenza di confini geografici[79].

La Convenzione è un trattato puramente "internazionale", innovativo e flessibile. Innanzitutto, i sessantotto Paesi firmatari[80] non sono solo membri del COE (Consiglio d'Europa) ma anche Paesi extraeuropei. Ciò ha consentito di accogliere concetti giuridici anche non europei, stimolare l'adesione di più Paesi, e aumentare così le probabilità di arrivare a un risultato il più possibile confacente con le diverse tradizioni giuridiche chiamate in gioco. Il carattere flessibile, invece, deriva dalla possibilità riconosciuta agli Stati di utilizzare mezzi e vie di cooperazione per raggiungere un accordo[81] e disciplinare un

---

[78] ARENA, *La convenzione di Budapest del consiglio d'Europa sulla repressione della criminalità informatica*, Catania, 2021 in cui l'Autrice afferma che Alexander Seger, Capo della Divisione della Criminalità informatica del Consiglio d'Europa, ha sottolineato che la Convenzione di Budapest rimanga, ad oggi, lo strumento internazionale più efficiente: "La Convenzione di Budapest è sinonimo di una visione di un Internet libero, dove le informazioni possono fluire liberamente, essere consultate e condivise, dove le restrizioni sono definite in modo restrittivo per contrastare l'uso improprio e dove vengono indagati e perseguiti solo reati specifici, fatte salve le necessarie garanzie".

[79] MATTARELLA, *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica*, in *Arch. pen*., 2022, fasc. 3, p. 45.

[80] Sul sito del Consiglio d'Europa*,* *https://www.coe.int/it/web/conventions/full-list*, è visionabile la lista degli Stati firmatari allo stato attuale e: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgio, Bosnia e Erzegovina, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Federazione Russa, Finlandia, Francia, Georgia, Germania, Gran Bretagna, Grecia, Irlanda, Islanda, Italia, Lettonia, Liechtenstein, Lituania, Lussemburgo, Malta, Monaco, Montenegro, Nord Macedonia, Norvegia, Paesi Bassi, Polonia, Portogallo, Repubblica Ceca, Repubblica di Moldavia, Repubblica Slovacca, Romania, San Marino, Serbia, Slovenia, Spagna, Svezia, Svizzera, Turchia, Ucraina, Ungheria, Argentina, Australia, Benin, Brasile, Burkina Faso, Canada, Capo Verde, Cile, Colombia, Costa Rica, Filippine, Ghana, Giappone, Guatemala, Israele, Marocco, Mauritius, Messico, Niger, Nigeria, Nuova Zelanda, Panama, Paraguay, Perù, Repubblica Dominicana, Senegal, Sri Lanka, Stati-Uniti d'America, Sud Africa, Tonga, Tunisia. Di questi, solo tre non hanno ratificato.
Inoltre, nel testo ufficiale, reperibile su *https://rm.coe.int,* all'articolo 36 "*Signature and entry into force*" si prescrive come condizione necessaria per l'entrata in vigore, la firma di cinque stati, tra i quali almeno tre devono essere membri del Consiglio d'Europa (« *This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2*»).

[81] Non sempre gli Stati sono riusciti ad accordarsi come, ad esempio, è accaduto con riguardo al reato di diffusione in rete di propaganda razzista. Vista la difficoltà nel trovare un punto di incontro a causa anche della complessità del problema, gli Stati avevano deciso di rinviare la questione al Comitato Europeo per i problemi della criminalità, il quale arrivò a predisporre un Protocollo addizionale alla Convenzione: Treaty NO. 189, "*Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*", firmato a Strasburgo nel 2003.

determinato aspetto del fenomeno. In particolare, il Comitato adibito alla preparazione della Convenzione aveva optato per la pubblicazione delle prime bozze, così che il dibattito negoziale tra Stati fosse stimolato e questi fossero sufficientemente informati, ma soprattutto la qualifica di "parte" nella negoziazione consentiva agli Stati di aggiungere protocolli e note di orientamento[82].

Per quanto riguarda i motivi che hanno portato a questo prodotto legislativo, merita sottolineare come l'obbiettivo fosse quello di raggiungere uno *standard* minimo di tutela per i beni giuridici e stabilire delle strategie minime volte al contrasto dei *computer crimes*, tenendo presente la natura transnazionale del fenomeno, cercando quindi di equilibrare le diverse strategie di tutela[83] previste da ciascuno degli ordinamenti e mirando a una politica comune. Il fine ultimo è non solo quello di tutelare la segretezza e l'integrità dei sistemi informatici ma anche contrastarne l'uso improprio e garantire un equilibrio tra quest'ultima esigenza e i diritti fondamentali, come, ad esempio, la libertà di espressione[84]. La Convenzione è inoltre caratterizzata da una forza applicativa che va oltre i cosiddetti "reati in senso proprio", comprendendo anche tutti quei reati che possono essere commessi mediante un sistema informatico o per i quali si richieda la raccolta di prove in forma elettronica (reati in senso lato)[85].

La Convenzione si divide in quattro capitoli: il capitolo uno è dedicato ai "*Use of terms*" (definizioni rilevanti); il capitolo due attiene alle "*Measures to be taken at the national level*" (misure da adottare in ambito nazionale); il capitolo tre si occupa dell'"*International co-operation*" (la cooperazione internazionale) e il capitolo quattro che conclude con le *"Final provisions*" (clausole finali)[86]. In totale la Convenzione si struttura di 48 articoli.

Il primo articolo fornisce definizioni terminologiche rilevanti volte all'armonizzazione di nozioni quali: "sistema informatico", con cui si fa riferimento a un apparecchio o gruppo di questi collegati e interconnessi che, mediante un programma, consentono un'automatica elaborazione di dati; "dati informatici", intesi come fatti, informazioni e concetti utilizzati dl programma per una determinata funzione; "fornitore di servizi", ossia un soggetto,

---

[82] ARENA, *op. cit.,* p.5.
[83] RESTA, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, *in Corriere del Merito*, Torino, 2008 in cui si legge «L'obiettivo primario della Convenzione sulla criminalità informatica risiede nell'esigenza di introdurre un minimum target di tutela dei beni giuridici offesi dai *cybercrimes* ed un livello minimo essenziale comune di strategie di contrasto a tali illeciti, soprattutto in ragione della loro natura tendenzialmente transnazionale, che comporta chiaramente la necessità dell'armonizzazione della relativa normativa di contrasto nell'ambito dei vari ordinamenti».
[84] Ciò si evince dal Preambolo della Convenzione consultabile sul sito *https://rm.coe.int.*
[85] PICOTTI, *Internet e diritto penale*, cit., p. 197 e FUMO, *op. cit.,* p. 772.
[86] Testo ufficiale consultabile in lingua inglese sul sito *https://rm.coe.int*.

pubblico o privato, che offre la possibilità ai propri utenti di comunicare con l'utilizzo di un sistema informatico o, ancora, colui preposto all'archiviazione o elaborazione di dati per contro del prestatore di servizi; e "dati relativi al traffico", ossia dati relativi a una comunicazione avvenuta mediante sistema informatico e prodotta da questo [87].

Con gli articoli successivi, nello specifico quelli contenuti al capitolo due, sezione prima, si entra nella parte della Convenzione dedicata al diritto sostanziale, che prevede misure legislative volte a contrastare le tipiche condotte illecite contro i sistemi informatici. La Convenzione ha introdotto dei "reati armonizzati"[88] con l'obbiettivo di evitare ipotesi di doppia incriminazione e stimolare una tutela e prevenzione migliori. L'elencazione di reati prevista in questa parte prende le proprie mosse dalla Raccomandazione del Consiglio d'Europa del 1989 e da altri studi portati avanti da diverse organizzazioni pubbliche e private[89].

Ai sensi dell'art. 11, paragrafo due, solo i reati indicati[90] nello stesso sono punibili a titolo di tentativo e questo perché molte delle fattispecie inserite nella Convenzione non sono concepibili in questa forma. Dall'altra parte, tutti i reati, ai sensi del paragrafo uno, sono punibili a titolo di concorso, purché vi sia l'elemento soggettivo della consapevolezza di star concorrendo alla commissione della fattispecie.

La prima categoria di reati comprende quelli contro la riservatezza, integrità e disponibilità di dati e sistemi informatici, quale l'accesso illegale, ex art. 2[91], in cui si sanziona la condotta di accesso abusivo, attuato senza autorizzazione e intenzionalmente, in un sistema informatico. È prevista anche la facoltà della Parte di richiedere che il reato

---

[87] Convenzione di Budapest, Art. 1: *« a) "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b) "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c) "service provider" means: i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service; d) "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service».*

[88] ARENA, *op. cit.,* p. 12.

[89] Esempi sono OCSE, ONU, AIDP.

[90] Convenzione di Budapest, Art. 11: *«2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention».*

[91] Illegal access: *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system».*

consista nella violazione di misure di sicurezza e con intenti illegali. Dal dettato dell'articolo emerge la necessarietà dell'abusività dell'accesso e dell'intenzione, rappresentando quindi un reato "ostacolo" volto a prevenire la commissione di reati più gravi[92]. L'intercettazione illegale ex art. 3[93] mira a tutelare la privacy e riservatezza dei dati informatici punendo l'intercettazione abusiva di trasmissioni non pubbliche[94]attuata con l'ausilio di appositi strumenti. L'attentato all'integrità dei dati e dei sistemi è incriminato agli artt. 4 e 5[95]. Il primo comprende tra le condotte illecite il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione, con la facoltà di ogni Stato di inserire quale ulteriore elemento del reato il grave danno[96]. L'art. 5 ricomprende le medesime condotte illecite, ma con l'obbiettivo di tutelare il funzionamento del sistema informatico. L'abuso di dispositivi è punito ai sensi dell'art. 6[97]: se da una parte la Convenzione ha optato per l'esclusione della punibilità di determinati fatti ritenuti non sufficientemente offensivi previsti nella lista facoltativa della Raccomandazione del 1989, come ad esempio il *Cybersquattage*, ha invece scelto di introdurre *ex novo*

---

[92] ARENA, *op. cit.,* p. 15.

[93] Illegal interception*: «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system».*

[94] ARENA, *op. cit.,* p. 16. L'aggettivo "non pubblico" qualifica la natura del processo di trasmissione dei dati e non la natura degli stessi.

[95] Data interference: *«1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration, or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm».*
System interference: *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data».*

[96] ARENA, *op. cit.,* p. 17. La gravità va ponderata in base alla legislazione nazionale di ciascuno Stato.

[97] Misuse of devices: *«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
*a) the production, sale, procurement for use, import, distribution or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1a.ii of this articles».*

l'articolo 6, anticipando notevolmente la rilevanza penale rispetto l'utilizzazione in concreto dei dispositivi e dati inserendo quale requisito il dolo specifico[98]. La norma punisce, infatti, non solo la fabbricazione, la vendita, la cessione, senza diritto, di dispositivi, software, password o codici validi per l'accesso al sistema, ma anche il mero possesso di tali strumenti, purché vi sia l'intenzione di utilizzarli al fine di commettere i reati di accesso abusivo o danneggiamento. Il legislatore nazionale dovrebbe cercare di specificare meglio questi elementi per determinare una soglia più decisa di punibilità[99].

La seconda categoria riguarda i reati informatici inseriti precedentemente nella lista minima della Raccomandazione del 1989 alle lettere a) e b). La falsificazione informatica ex art. 7[100] mira a sanzionare condotte strumentali come «introduzione, alterazione, cancellazione o soppressione (...) di dati informatici rispetto al risultato di creare dati non autentici, nell'intenzione che essi siano considerati o utilizzati a fini giuridici come se fossero autentici»[101]. I dati a contenuto probatorio rappresentano l'oggetto della disposizione, al fine di tutelare la certezza delle prove e la sicurezza di quei dati preposti alla disciplina legale dei rapporti[102]. La frode informatica, di cui all'art. 8[103], sanziona due diverse condotte, ossia «l'introduzione, alterazione, cancellazione o soppressione di dati informatici» e «ogni interferenza nel funzionamento di un sistema informatico», volte alla determinazione di un pregiudizio nella sfera patrimoniale altrui ovvero un beneficio economico proprio o di terzi.

Una terza categoria di reati, successivamente estesa con il Protocollo firmato a Strasburgo nel 2003[104], è quella relativa al contenuto. La pornografia infantile, prevista all'art. 9[105], è norma che assume particolare rilievo nell'ambito della Convenzione, come si

---

[98] PICOTTI, *Internet e diritto penale*, cit., p. 199.
[99] In tal senso PICOTTI, *Ivi.*, p. 200 e ARENA, *op. cit.,* p. 19.
[100] Computer-related forgery: *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches».*
[101] PICOTTI, *Internet e diritto penale*, cit., p. 200.
[102] ARENA, *op. cit*., p. 20.
[103] Computer-related fraud: *«Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion, or suppression of computer data, b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person».*
[104] Treaty NO. 189, "*Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*", firmato a Strasburgo nel 2003.
[105] Offences related to child pornography: *«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through*

evince dal fatto che ricopre l'intero Titolo III della stessa, potendosi anche applicare ad altri illeciti simili[106] . La definizione di "pornografia minorile" è stata introdotta successivamente rispetto alla Convenzione grazie alla Direttiva 2011/92/UE del Parlamento Europeo e Consiglio[107], fugando così ogni altra possibile interpretazione. La Convenzione sui diritti dell'infanzia approvata dall'Assemblea generale delle Nazioni Unite, entrata in vigore nel 1990, ex art. 1, stabilisce che per minore si deve intendere il soggetto con età inferiore ai diciotto anni, tuttavia, ciascuno Stato può eventualmente prevedere una soglia diversa purché non inferiore all'età di sedici anni[108]. La disposizione fa rientrare nel "materiale pornografico": quello in cui viene raffigurato un minore in comportamenti sessualmente espliciti (paragrafo 2, lett. a); la pornografia virtuale (paragrafo 2, lett. b); la pornografia apparente (paragrafo 2, lett. c)[109]. Nei casi alle lett. a) e c), i beni giuridici tutelati oggetto sono rappresentati non tanto dalla tutela del minore rispetto allo sfruttamento al fine di produrre materiale pornografico, quanto del tentativo di impedire comportamenti prodromici a questi fini volti all'incoraggiamento e reclutamento dei minori[110]. Vengono sanzionate le condotte di produzione di pornografia minorile allo scopo della diffusione, l'offerta, la distribuzione, il procacciamento per sé o per altri e il possesso mediante un sistema informatico di tale materiale.

---

*a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub- paragraphs d and e, and 2, sub-paragraphs b and c».*

[106] PICOTTI, *Internet e diritto penale*, cit., p. 201.

[107] (9) "La pornografia minorile comprende spesso la registrazione di abusi sessuali compiuti sui minori da parte di adulti. Essa può anche comprendere immagini di minori coinvolti in atteggiamenti sessuali espliciti o immagini dei loro organi sessuali, ove tali immagini siano prodotte o utilizzate per scopi prevalentemente sessuali, indipendentemente dal fatto che siano utilizzate con la consapevolezza del minore. Inoltre, il concetto di pornografia minorile comprende altresì immagini realistiche di un minore in atteggiamenti sessuali espliciti o ritratto in atteggiamenti sessuali espliciti, per scopi prevalentemente sessuali", definizione visionabile nel testo ufficiale della Direttiva nel sito della Gazzetta Ufficiale dell'Unione Europea.

[108] Convenzione ONU sui diritti dell'infanzia, Art. 1: «Ai sensi della presente Convenzione si intende per fanciullo ogni essere umano avente un'età inferiore a diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile».

[109] ARENA, *op. cit*., p. 23. Per pornografia apparente si intende "immagini realistiche rappresentanti un minore impegnato in un comportamento sessualmente esplicito", senza che sia realmente coinvolto. Mentre, la nozione di comportamenti espliciti fa riferimento a "una persona che appaia come un minore impegnato in un comportamento sessualmente esplicito".

[110] PICOTTI, *Internet e diritto penale*, cit., p. 202.

Infine, vi è la categoria dei reati contro la proprietà intellettuale e diritti collegati enucleati all'art.10[111] il quale non descrive condotte precise, ma rinvia alle legislazioni nazionali escludendo i marchi e brevetti dalla Convenzione in quanto non indicati espressamente.

Ciò che accomuna tutte queste fattispecie di reato, ad eccezione di quella riguardante il diritto d'autore, è la presenza di due elementi, uno oggettivo e uno soggettivo: il primo consiste nella necessità che la condotta avvenga "senza diritto", mentre il secondo è rappresentato dal dolo, il cui contenuto verrà precisato dalle legislazioni interne[112].

Un'altra disposizione importante è quella prevista all'art. 13[113] la quale dispone che l'efficacia di tali fattispecie deve essere assicurata mediante sanzioni effettive, proporzionate e dissuasive, che annoverino finanche la privazione della libertà.

L'Italia, già con la legge n. 547/1993, sulla base di ciò che era stato disposto dalla Raccomandazione (89) 9 del 1989, aveva proceduto a incriminare certe condotte inserite nella Convenzione, tra queste: la frode informatica di cui all'art. 640-ter c.p.; l'accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p.; danneggiamento di cui all'art. 635-*bis* c.p.; intercettazione riconducibili agli artt. 617-*quater* e 617-*quinquies* del c.p.; abuso di apparecchiature ex art. 615-*quater* del c.p.

---

[111] Offences related to infringements of copyright and related rights: *«1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article».*

[112] PICOTTI, *Ivi.*, p. 198.

[113] Sanctions and measures: *«1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate, and dissuasive sanctions, which include deprivation of liberty.*
*2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate, and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions».*

La seconda sezione del capitolo due della Convenzione, artt. 14- 21[114], ha ad oggetto la parte di diritto processuale comune: trattasi della parte su cui si sono concentrate maggiormente le critiche essendo il tema per cui è stato necessario trovare un equilibrio tra l'esigenza di migliorare gli strumenti di tutela contro le aggressioni informatiche e la tutela delle libertà individuali e privacy[115]. La disciplina punta soprattutto ad introdurre modalità di conservazione dei dati in virtù di una loro futura utilizzazione nell'ambito di un procedimento.

Il terzo capitolo riguarda la cooperazione internazionale e mira a migliorare la capacità investigativa degli Stati cercando di consentire uno scambio di informazioni fluido e rapido e rendere le indagini che riguardano più Stati efficienti, trovando un accordo tra le legislazioni nazionali. Questo obbiettivo emerge dal dettato dell'art. 23[116] in cui si richiede agli Stati di collaborare il più possibile nell'ambito delle indagini o nella raccolta di prove elettroniche, sempre nel rispetto di ciò che è previsto in questo stesso capitolo, degli strumenti di cooperazione internazionale e accordi stipulati. Questo capitolo comprende un titolo rivolto ai principi generale sull'estradizione[117], istituto che si basa sul principio della

---

[114] Art 14- *Scope of procedural provisions* (Ambito di applicazione delle disposizioni procedurali); Article 15 – *Conditions and safeguards* (condizioni e tutele); Article 16 – *Expedited preservation of stored computer data* (Conservazione accelerate dei dati informatici memorizzati); Article 17 – *Expedited preservation and partial disclosure of traffic data* (Conservazione e divulgazione rapida dei dati relativi al traffico); Article 18 – *Production order* (Ingiunzione di produrre); Article 19 – *Search and seizure of stored computer data* (Perquisizione e Sequestro dei dati immagazzinati); Article 20 – *Real-time collection of traffic data* (Raccolta in tempo reale di dati sul traffico); Article 21 – *Interception of content data* (Intercettazione di dati relativi al contenuto).

[115] ARENA, *op. cit*., p. 27.

[116] General principles relating to international co-operation: *«The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co- operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence».*

[117] Article 24 – Extradition: *«1. a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2. The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence 4. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the*

"doppia criminalità"[118], quindi l'esigenza che la condotta sia qualificata come reato in entrambe legislazioni nazionali cercando di risolvere le problematiche riconducibili allo strumento. Il titolo tre, invece, si occupa di enucleare i principi volti a disciplinare la cosiddetta mutua assistenza, in particolare artt. 25 e 26, principio fondamentale per garantire celerità nei procedimenti e nelle indagini quando coinvolti sistemi informatici. Sempre con l'obbiettivo di snellire le procedure, la Convenzione ha inserito una serie di misure (artt. 29-35) come, ad esempio, la rapida divulgazione dei dati di traffico conservati[119] o l'assistenza concernente l'accesso ai dati raccolti[120].

Infine, il quarto capitolo, che va dagli artt. 36- 48, contiene delle disposizioni conclusive in materia di adesione, firma, ambito di applicazione e ancora riserve riconosciute agli Stati.

La Convenzione ha rappresentato lo strumento per cercare di arrivare alla creazione di una politica comune tra Stati, come miglior modo per affrontare la natura transfrontaliera del fenomeno di criminalità informatica ed evitare la creazione di "paradisi informatici", in cui non sono previste le tutele minime garantite dalla Convenzione.

---

*person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7. a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval, or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times».*

[118] ARENA, *op. cit*., p. 42.

[119] Article 30 – Expedited disclosure of preserved traffic data: *«1. Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2. Disclosure of traffic data under paragraph 1 may only be withheld if: a) the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b) the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests».*

[120] Article 31 – Mutual assistance regarding accessing of stored computer data: *«1. A Party may request another Party to search or similarly access, seize, or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2. The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.3. The request shall be responded to on an expedited basis where: a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation».*

## 2.4. La Legge n. 48/2008 di ratifica ed esecuzione della Convenzione "*Cybercrime*".

La Convenzione di Budapest è stata poi ratificata, non senza ritardo, dal legislatore italiano con la presentazione alle Camere del D.D.L n. 2807 nel giugno del 2007, trasformato poi nella Legge n. 48 di "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" il 18 marzo del 2008.

L'*iter* legislativo che ha portato al venire in essere di questo prodotto legislativo, considerato disastroso[121], è stato particolarmente travagliato. Nel 2003, su sollecitazione del rappresentante del Ministro della Giustizia che aveva partecipato alle attività di preparazione dello schema di Convenzione, venne istituita una Commissione Interministeriale con lo scopo di redigere uno schema di legge di ratifica della Convenzione. Negli anni 2004-2005 le iniziative legislative in materia di diritto penale dell'informatica furono caratterizzate da un forte scoordinamento. Questo emerse, ad esempio, dalla istituzione della Commissione Nordio, incaricata di elaborare un nuovo testo del Codice penale. Il progetto che venne presentato voleva apportare alcune modifiche alla parte speciale del Codice, relativa ai reati informatici, introdotti dalla Legge del 1993: una simile iniziativa risultava non solo non giustificata, ma anche poco coerente e superflua vista l'istituzione della Commissione Interministeriale e l'attività ad essa assegnata[122].

Il lavoro della Commissione Interministeriale si concluse nel 2004 con l'elaborazione di uno schema volto sia alla modifica di alcuni articoli del Codice penale, quali gli artt. 420, 491, 491 *bis*, 615 *ter* e *quinques,* 617 *quater* e *quinques,* 635 *quater*, all'introduzione di nuove fattispecie come quelle previste agli artt. 600 *octies*, 600 *nonies*, 635 *ter* e *quater,* nonché alla modifica di disposizioni del c.p.p. e del D. Lgs n. 231 del 2001[123]. L'*iter* che ha portato al progetto finale in realtà è stato particolarmente rapido. Esso si è svolto in un totale di cinque sedute nei due rami del Parlamento, nel corso delle quali sono state avanzate osservazioni che hanno ampiamente mostrato la scarsa conoscenza dei parlamentari con riguardo al tema[124], tanto da avanzare la proposta di avvalersi delle consulenze di esperti

[121] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., p. 632.
[122] ID, *Sicurezza informatica e lotta alla cibercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislati*ve, in *Dir. Internet*, 2005, fasc. 5., p. 437.
[123] ID, *Informatica, internet e diritto penale*, cit., p. 633.
[124] Ad esempio, nella seconda seduta, l'on. Costa dichiarò che «l'attuale normativa risaliva al 1993 ed era stata adottata sulla base di una situazione emergenziale e senza alcun coordinamento internazionale…». Lo stesso Autore, SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., p. 635, che ha partecipato attivamente ai lavori preparatori del disegno di legge che ha portato alla promulgazione della novella del 1993, afferma di non essere in grado di capire quale sia questa situazione di emergenza. La confusione dell'Autore

nelle materie trattate dal disegno di legge. Al termine delle sedute, il 4 aprile del 2008, la Legge n. 48 fu pubblicata in Gazzetta ufficiale ed entrò in vigore il giorno seguente. La rapidità con cui si è arrivati a questa legge è stato il frutto del bilanciamento tra le esigenze di adeguamento veloce dell'ordinamento italiano alla Convenzione di Budapest e di elaborazione una novella legislativa accurata. Facendo prevalere la prima di queste esigenze, il prodotto legislativo ne uscì caratterizzato da diverse incongruenze nella speranza che poi la magistratura avrebbe risolto le problematiche in sede interpretativa[125].

La legge si compone di quattro capitoli per un totale di quattordici articoli. L'art. 2 dispone che "Piena e intera esecuzione è data alla Convenzione, a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall'articolo 36 della Convenzione stessa" affermazione che stride poi con l'effettiva fattura delle disposizioni di diritto sostanziale e processuale inserite nell'ordinamento italiano[126].

Concentrandosi sulla parte di diritto sostanziale, gli artt. 3- 7[127] del Capo II, intitolato "Modifiche al Codice penale e al decreto legislativo 8 giugno 2001, n. 231", inseriscono o

---

si estende anche all'affermazione "senza alcun coordinamento internazionale" dato che dalla relazione di accompagnamento del disegno di legge n. 2773, consultabile sul sito *https://www.penale.it*, si legge esplicitamente «Un ulteriore aspetto problematico e connesso alla necessità di adeguare la legislazione italiana alle direttive impartite da organismi sopranazionali cui l'Italia aderisce. Nella materia dei reati informatici il Consiglio d'Europa ha proposto due diverse liste di reati da introdurre, una «minima» e l'altra facoltativa: occorreva operare una scelta e, come si vedrà, si è ritenuto di non poter limitare la previsione dei nuovi reati alla prima».

[125] PICOTTI, *I profili di diritto sostanziale*, in *La ratifica della Convenzione Cybercrime del Consiglio d'Europa*, in *Dir. pen. proc*., 2008, fasc. 6, p. 700.

[126] PICOTTI, *Ivi*., p. 701 e ID, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. Internet*, 2008, fasc. 5, p. 437.

[127] Art. 3- Modifiche al titolo VII del libro secondo del Codice penale: «1. All'articolo 491-bis del Codice penale sono apportate le seguenti modificazioni: a) al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»; b) il secondo periodo è soppresso. 2. Dopo l'articolo 495 del Codice penale è inserito il seguente: «Art. 495-bis. - (Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri). - 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 fino ad un anno».
Art. 4- Modifica al titolo XII del libro secondo del Codice penale: «1. L'articolo 615-*quinquies* del Codice penale è sostituito dal seguente: «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».
Art. 5- Modifiche al titolo XIII del libro secondo del Codice penale: «1. L'articolo 635-*bis* del Codice penale è sostituito dal seguente: «Art. 635-*bis*. - (Danneggiamento di informazioni, dati e programmi informatici). - 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 sei mesi a tre 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 della reclusione da uno a quattro anni e si procede d'ufficio». 2. Dopo l'articolo 635-*bis* del Codice penale sono inseriti i seguenti: «Art. 635-*ter*. - (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente

modificano fattispecie che in realtà non sembrano essere attuative della Convenzione ma bensì frutto di una scelta autonoma del legislatore, il quale ha visto la legge di ratifica come uno strumento per revisionare parti di norme già vigenti. Un esempio in tal senso sono gli artt. 495 *bis* c.p. e 640 *quinques* c.p. con i quali sono state introdotte due nuove fattispecie: la falsa dichiarazione o attestazione al certificatore di firma elettronica e la frode informatica del soggetto che presta servizi di certificazione di firma elettronica, due figure che non risultano essere riconducibili allo strumento internazionale e che puniscono condotte volte alla violazione delle previsioni in materia di firma elettronica[128]. La figura prevista all'art.

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 grave- mente 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 danneggia- mento 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». 3. Dopo l'articolo 640-quater del Codice penale è inserito il seguente: «Art. 640-*quinquies.* - (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica). - 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 fino a tre anni e con la multa da 51 a 1.032 euro».
Art. 6- Modifiche all'articolo 420 del Codice penale: «1. All'articolo 420 del Codice penale, il secondo e il terzo comma sono abrogati».
Art. 7- Introduzione dell'articolo 24-bis del decreto legislativo 8 giugno 2001, n. 231: 1. Dopo l'articolo 24 del decreto legislativo 8 giugno 2001, n. 231, è inserito il seguente: «Art. 24-bis. - (Delitti informatici e trattamento il- lecito di dati). - 1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del Codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote. 2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del Codice penale, si applica all'ente la sanzione pecuniaria sino a tre- cento quote. 3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del Codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote. 4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previ- ste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lette- re c), d) ed e)».

[128] PICOTTI, *I profili di diritto sostanziale*, cit., p. 704. Per approfondimenti si veda SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., p. 648.

640 *quinques* è stata maggiormente criticata[129] in quanto non pare essere idonea a configurare il paradigma tipico dei reati di truffa venendo a mancare non solo la condotta fraudolenta, essendo sufficiente la violazione di obblighi extra penali[130] e lo specifico intento del soggetto, ma anche l'elemento patrimoniale che connota i delitti contro il patrimonio.

Un'altra modifica di non poca importanza ha interessato l'art. 491 *bis* c.p., di cui è stato abrogato il secondo periodo[131]. Infatti, in base a ciò che emerge dalla Relazione di accompagnamento al D.D.L n. 2807, si è optato per accoglimento di una più ampia definizione di "documento informatico", come utilizzata nell'ambito del D.P.R n. 513 del 1997 recante i criteri e le modalità per la trasmissione, archiviazione e formazione di documenti con strumenti informatici o telematici, intesa come "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"[132].

Le norme che effettivamente hanno attuato il capitolo due della Convenzione sono tre: l'art. 4, che ha sostituito l'originaria formulazione dell'art. 615 *quinques* c.p. cercando di renderlo più coerente con l'art. 6 della Convenzione; l'art. 5, con cui si è modificato l'art. 635 *bis* in materia di danneggiamento di dati introducendo anche nuove fattispecie, quali gli artt. 635 *ter, quater* e *quinques* c.p; e l'art. 6, con cui si sono abrogati i commi due e tre dell'art. 420 c.p. che sanzionavano ipotesi di attentato ad impianti di pubblica utilità relativi a sistemi informatici[133].

Le modifiche apportate alla parte di diritto sostanziale si concludono con l'art. 7, il quale, in linea con gli artt. 12 e 13, paragrafo due, della Convenzione e la Decisione UE 2005/222/GAI, ha integrato il d.lgs n. 231 del 2001 aggiungendo l'art. 24 *bis* con lo scopo di estendere la responsabilità amministrativa da reato delle persone giuridiche ed enti a quasi tutte le fattispecie di reato informatico. A riguardo, destano alcuni dubbi sia l'esclusione dell'art. 640 *ter* c.p. quando commesso in danno dello Stato o di altro ente pubblico, continuando ad applicarsi l'art. 24 del d.lgs del 2001 nella sua originale versione, che

---

[129] In tal senso SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 652 e PICOTTI, *I profili di diritto sostanziale,* cit., 706, in base al quale nel caso dell'attività di certificazione potrebbero non ricorrere le condotte di "alterazione del funzionamento di un sistema" o di "intervento senza diritto su dati, informazioni o programmi".

[130] Previsti all'art. 32, comma due ss, del Codice dell'Amministrazione digitale.

[131] In cui si leggeva, quale definizione di documento informatico, «qualunque supporto contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». Gli Autori AMATO-DESTITO-DEZZANI-SANTORIELLO, in *I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, Padova, 2010, p. 28, hanno sottolineato l'inadeguatezza di questa definizione, la quale appariva ignorare non solo la possibilità di tener separati i dati dal loro supporto materiale, ma anche il tipo di efficacia probatoria da attribuire. Per approfondire si veda PICOTTI, R*atifica della Convenzione Cybercrime e nuovi strumenti di contrasto*, cit., p. 439 e ID., *La ratifica della Convenzione Cybercrime*, cit., p. 701.

[132] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., p. 644.

[133] PICOTTI, R*atifica della Convenzione Cybercrime e nuovi strumenti di contrasto*, cit., p. 438.

l'esclusione dell'art. 495 *bis* c.p. il quale risulta suscettibile di essere commesso nell'interesse di una persona giuridica[134].

Dal punto di vista processuale, la Legge n. 48 si è occupata agli artt. 8, 9 e 11, dell'integrazione di alcune disposizioni del c.p.p. mirando ad un adeguamento lessicale, così da chiarire l'applicazione al fenomeno informatico di istituti processuali già vigenti nel Codice. Da un lato, il legislatore si è limitato ad inserire precisazioni, come ad esempio "misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" al secondo comma dell'art. 244 c.p.p. o, ancora, che la copia dei dati debba avvenire "mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità" *ex* artt. 260, comma due e 354, comma due, c.p.p. Dall'altro, si è proceduto all'estensione delle attività di ricerca ed acquisizione di mezzi di prova come nel caso del sequestro di corrispondenza che è stato esteso anche a quella telematica *ex* art. 254 comma uno e due c.p.p. e ad "altri dati presso fornitori di servizi informatici, telematici e di telecomunicazioni" *ex* art. 254 *bis* c.p.p., sempre prevedendo come modalità di acquisizione la loro duplicazione su di un adeguato supporto volto a garantirne la conservazione e protezione[135]. Invece, l'art. 10 ha introdotto uno strumento processuale innovativo, ossia la "conservazione rapida dei dati" come prevista all'art. 16 della Convenzione comportando alcune modifiche al decreto legislativo 30 giugno 2003, n. 196[136].

Come già premesso, il prodotto che è derivato dall'attività della Commissione Interministeriale è stato deludente, perché presenta incongruenze e frettolosità che non avrebbero dovuto caratterizzare una legge così importante in quanto attuativa della Convenzione. La dottrina ha concordemente affermato che la legge di ratifica rappresenti "un intervento solo parziale e frammentario, in cui l'urgenza vada a scapito della qualità tecnica e sistematica della normativa interna, non garantisce affatto il raggiungimento delle finalità d'armonizzazione legislativa e di rafforzamento della cooperazione internazionale fra gli Stati e le loro autorità inquirenti e giudicanti, che costituiscono la ragion d'essere degli strumenti internazionali"[137].

---

[134] PICOTTI*, Ivi*, p. 447.
[135] PICOTTI*, Ivi*, p. 448 e LUPÀRIA, *I profili processuali*, in *La ratifica della Convenzione Cybercrime*, cit., p. 719 ss.
[136] Dalla Relazione di accompagnamento del D.D.L n. 2807 emerge come solo in questo caso vi sia stato l'inserimento *ex novo* di fattispecie nel c.p.p.
[137] SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, cit., p. 668 e PICOTTI, *Profili di diritto sostanziale,* in *La ratifica della Convenzione Cybercrime*, cit., p. 716.

# CAPITOLO II

# LE FRODI *ONLINE*: IL REATO DI FRODE INFORMATICA (ART. 640 *TER* C.P.) E IL *PHISHING*

SOMMARIO: 1. La nuova fattispecie di frode informatica e i possibili modelli di tutela. - 1.1. Il bene giuridico oggetto del reato di frode informatica. - 1.2 Le due modalità di condotta: l'alterazione del funzionamento di un sistema informatico o telematico e l'intervento senza diritto su dati, informazioni o programmi. - 2. La fattispecie di utilizzazione indebita di carte di credito o di pagamento *ex* art 493 *ter* c.p. - 3. La nuova variante del "*Phishing"*.

## 1. La nuova fattispecie di frode informatica e i possibili modelli di tutela.

L'aumento delle possibili operazioni eseguibili mediante *computer* e l'avvento delle interconnessioni globali su rete tra diversi sistemi hanno rappresentato un'agevolazione per il soggetto che decida di sfruttare le capacità operative dell'operatore informatico per assicurarsi un profitto a danno del soggetto passivo[1].

Fra le ipotesi criminose che si possono verificare nel settore bancario, a titolo di esempio, si annovera il dipendente che manipola l'archivio dei dati della banca con il fine ultimo di accreditare sul proprio conto corrente piccole quantità di denaro o percentuali di interessi, procurandosi così, con diverse operazioni, ingenti profitti[2]. Le innumerevoli vie d'azione percorribili consentono al soggetto agente di poter utilizzare non solo i sistemi operativi propri delle banche, ma anche di enti pubblici, come l'I.N.P.S[3] o di società per procurarsi rapidamente un profitto, nella convinzione di rimanere nell'anonimato.

Inoltre, la diffusione delle applicazioni di *home banking*[4] e la conseguente tendenza a ricorrervi hanno reso fertile il terreno per coloro che intendono introdursi nelle

[1] SCOPINARO, in *Internet e reati contro il patrimonio*, Torino, 2007, p. 33.
[2] Si veda in particolare PELLEGRINI, *Uso non autorizzato del computer. Limiti e prospettive della tutela penale*, in *Dir. inform*, 1987, p. 289 ss.
[3] Un esempio, utilizzato in MARCELLI, *I reati informatici a danno dell'istituto nazionale della previdenza sociale (I.N.P. S)*, in *Dir. inform*, 1993, fasc. 4-5, p. 1007 e oggetto della sentenza del Trib. Roma, 20 giugno 1985, ha riguardato il caso di un intervento svolto sui dati archiviati nel sistema centrale dell'istituto che ha portato a rappresentare falsamente l'avvenuto accredito di versamenti contributivi.
[4] PICA, in *Diritto penale delle nuove tecnologie informatiche: computer's crimes e reati telematici internet banche dati e privacy*, Torino, 1999, p.140 con il termine "*home banking*" fa riferimento a quelle operazioni telematiche volte all'agevolazione di operazioni economiche, le quali consentono al cliente di compiere quest'ultime dal proprio domicilio senza la necessità di recarsi fisicamente in banca.

comunicazioni telematiche altrui al fine di carpire codici di accesso e credenziali (come *username* e *password*) e usufruire di servizi *online*[5].

Sin dai primi momenti in cui si sono verificate truffe mediante l'ausilio delle tecnologie è emersa l'inadeguatezza della normativa penale. In particolare, si erano riscontrate forti difficoltà nell'accertare l'esistenza di taluni elementi costituivi del reato di truffa *ex* art. 640 c.p., quali l'induzione in errore (spesso, infatti, ciò che veniva ingannato era un *personal computer* e non una persona fisica) o l'atto di disposizione patrimoniale[6]. Vi sono stati poi dei casi, come quello che ha visto un dipendente bancario inserire dei dati per rappresentare falsamente l'effettuazione di versamenti in contanti anziché in assegni, nei quali è stata riconosciuta la configurabilità della truffa aggravata: il giudice di primo grado, nel caso concreto, aveva ritenuto sussistente la condotta di artifici e raggiri volti a trarre in inganno gli organi della banca preposti al controllo[7].

Queste difficoltà interpretative sono dovute alla trasformazione tecnologica, che ha portato ad una modifica delle modalità di aggressione proprie della truffa e del furto e ha reso sempre più complessa per gli interpreti l'attività di adeguamento della normativa al nuovo fenomeno.

Con riguardo alla truffa, se prima questa era caratterizzata dalla presenza, quale elemento implicito, della cooperazione della vittima nella forma dell'atto di disposizione patrimoniale, successivamente, ha subito una forte spersonalizzazione. Questa metamorfosi ha impattato su due versanti. In primo luogo, sull'oggetto della tutela: inizialmente questo si poteva agevolmente individuare nella libertà di disposizione patrimoniale della vittima, ora, invece, si può ricondurre all'affidamento che la persona offesa ripone sulle dichiarazioni del proprio interlocutore. In secondo luogo, molto spesso l'autore del reato si trova a interfacciarsi con un sistema informatico e non più con una persona fisica specifica e ben determinata[8]: quest'ultimo effetto ha inciso sulla difficoltà per interpreti nel riconoscimento dell'elemento dell'induzione in errore. A riguardo, si è parlato di un paralogismo: il *computer* opera mediante il cosiddetto *software,*[9] consistente nella rappresentazione di ciò

[5] Ad esempio, fare ricorso al modo dell'*e-commerce* e utilizzare la carta di credito di un terzo soggetto inconsapevole per comprare beni in vendita su siti *web*.
[6] DESTITO- DEZZANI- SANTORIELLO, in *Il diritto penale delle nuove tecnologie*, Milano, 2007, p. 58.
[7] Trib. Roma, 14 dicembre 1985, in *Dir. inform*, Milano, 1988, p. 487.
[8] BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. inform*., 2011, fasc. 3, p. 385.
[9] AMATO MANGIAMELI, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica*, in *I reati informatici. Elementi di teoria generale e principali figure criminose*, a cura di AMATO MANGIAMELI-SARACENI, Torino, 2015, p. 36 definisce il *software* come bene non-rivale è, paragonandolo alla conoscenza umana, lo qualifica come cumulativo e modulare. Una definizione la si rinviene anche nella relazione governativa di accompagnamento al disegno della legge n. 547 del 1993, consultabile sul sito

che è voluto dall'utente; di conseguenza, alterare il sistema informatico o manipolarlo equivale a trarre in inganno lo stesso utente che sta facendo uso del *computer*[10]. Nonostante questa ricostruzione, i dubbi interpretativi non sono stati fugati, potendosi obbiettare che in virtù del divieto di analogia in materia penale questa rappresenterebbe una forzatura giuridica inaccettabile[11].

Anche le modalità di realizzazione della condotta di furto sono state modificate dall'evoluzione tecnologica, ma, all'inverso, nel senso di una valorizzazione della persona. In particolare, ferma la tendenza a dare rilevanza al rapporto che intercorre tra la persona offesa e la cosa mobile oggetto del reato, è diventata altrettanto importante la relazione tra reo e vittima[12]. Rimane comunque salva la considerazione, anche in questo caso, che il furto rappresenti un tipo di reato spersonalizzato, sia per l'unilateralità dell'aggressione sia per l'assenza di un rapporto diretto con la vittima[13].

È apparsa, quindi, subito opportuna la tipizzazione delle nuove forme di criminalità[14]. Il legislatore del '93, sulla scorta di quello europeo del 1989, seguendo la via della ricostruzione dei reati informatici come lesivi di beni classici, e quindi senza una vera e propria autonomia, ha dovuto decidere se strutturare la frode informatica sul modello della truffa oppure del furto con destrezza[15]. L'alternativa si basa sulla visione adottata: qualora si dovesse concordare con una visione "antropomorfica", il disvalore del reato sarà incentrato sull'inganno attuato nei confronti del *computer* e si prediligerà la prima opzione.

---

*http://legislature.camera.it,* p. 2 in cui si legge "il *software*, sia esso di base, di supporto, generalizzato o applicativo, inglobando del concetto qualunque programma informatico realizzato dal costruttore dell'*hardware*, da strutture di produzioni *ad hoc*, da singoli utenti e registrato sui supporti più vari, dal singolo semiconduttore ai supporti di memorizzazione magnetici, ottici o di altra natura".

[10] PICA, *op. cit*., p. 140 e BORRUSO- BUONOMO- CORASANTI- D'AETTI, *Profili penali dell'informatica*, Milano, 1994, p. 35.

[11] Relazione di accompagnamento al disegno di legge n. 2773, convertito poi nella Legge n. 547 del 1993, consultabile sul sito *https://www.penale.it.*

[12] A prova di questa tendenza, BARTOLI, *op. cit*., p. 386, si riferisce alle riforme volte a valorizzare il rapporto della vittima con la cosa mobile come, ad esempio, la previsione del reato autonomo di furto con strappo o, ancora, l'introduzione di nuove circostanze del fatto commesso nei confronti del soggetto che sia fruendo o, comunque, abbia già fruito dei servizi di istituti di credito *ex* art. 625, comma 1, n. 8 ter c.p.

[13] BARTOLI, *op. cit*., p. 385.

[14] Urgenza che è stata espressa chiaramente, nella Relazione governativa che ha accompagnato il disegno di legge n. 2773, nel seguente passaggio: "La discussa configurabilità del reato di truffa (art. 640 c.p.) in caso di analogo illecito «informatico», in particolare come s'è detto per l'aspetto attinente all'induzione in errore, impone per detto illecito la creazione di una nuova figura di reato (art. 10) nella quale la comune condotta di artificio o raggiro è più specificamente integrata dall'alterazione di un sistema informatico o telematico o dall'abusivo intervento con ogni mezzo effettuato su dati, informazioni o programmi contenuti in detti sistemi".

[15] SCOPINARO, *op. cit.,* p. 46 in cui si legge che la *ratio*, alla base dell'introduzione nel Codice penale dell'art. 640 *ter*, è stata la necessità di prevedere una tutela e sanzione per quei fatti realizzati per profitto mediante tecnologie. Al riguardo, la dottrina ha per tempo discusso se la norma dovesse richiamare il modello di tutela previsto per la truffa, *ex* art. 640 c.p., oppure del furto con destrezza, *ex* art. 624 in combinato disposto con art. 625 n. 2 c.p.

Questa è, infatti, una ricostruzione che si basa sull'equivalenza tra *computer* e persona fisica[16]; diversamente, se si seguisse la visione "antropocentrica", che sostiene l'unilateralità dell'aggressione della frode informatica, sarebbe inevitabile prediligere il reato di furto quale parametro da seguire[17].

Il legislatore si è trovato a dover scegliere tra questi due diversi modelli di tutela contro la frode informatica: in base al primo, strutturato sulla falsariga della truffa, facendo leva sulla circostanza per la quale, nel caso di interazione con un sistema informatico che porta al conseguimento di un profitto grazie alle operazioni che il soggetto ha fatto compiere al sistema, l'autore non realizza una condotta di sottrazione con impossessamento di cosa mobile altrui. L'assenza di un bene suscettibile di sottrazione ha reso impossibile l'applicazione della norma sul furto[18]; il secondo, invece, modellato sullo schema del furto vista la questione del difficile riconoscimento dell'elemento dell'induzione in errore[19] per poter applicare il reato di truffa. Sotto il punto di vista della condotta, quindi, sarebbe risultata più confacente la struttura del furto.

Con la novella del 1993 il legislatore ha optato per l'inserimento del nuovo art. 640 *ter* nel Capo II del Titolo XIII del Codice penale - dedicato ai "Delitti contro il patrimonio mediante frode" - il quale prevede al comma uno 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 da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro»[20].

A differenza del legislatore italiano, altri Paesi hanno previsto la necessaria concretizzazione di tre diversi eventi che compongono l'aggressione: la manipolazione del

---

[16] BARTOLI, *op. cit.,* p. 384.

[17] *Ibidem,* l'Autore parla al riguardo di "ambivalenza" della frode informatica con il rischio annesso che questa caratteristica possa portare a una vera ambiguità e a un conseguente disorientamento della giurisprudenza.

[18] L'inapplicabilità dell'art. 624 c.p. è stata ribadita da GIANNANTONIO, *I reati informatici*, in *Dir. Inform*., 1992, fasc. 3, p. 380.

[19] PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, p. 40 in cui si legge "nei casi di manipolazione dei dati l'operatività della figura della truffa non poteva escludersi del tutto, ma risultava fortemente condizionata dalle circostanze del caso". Infatti, il computer non viene ingannato, ma utilizzato per dare avvio a un'operazione che gli porti un vantaggio patrimoniale.

[20] L'articolo si compone di quattro commi e gli ultimi tre recitano: "La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Il delitto è punibile a querela [120-126] della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o la circostanza prevista dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età".

sistema informatico; l'effetto che deriva da questa condotta fraudolenta, inteso come l'alterazione del prodotto dell'operatore informatico; il danno patrimoniale e il profitto ingiusto[21]. Da questa ricostruzione del reato emerge, innanzitutto, che ciò che rileva è la circostanza che venga realizzata un'interferenza che vada ad impattare in modo diretto, ma anche indiretto, sull'elaborazione dei dati. Inoltre, il fatto che il danno patrimoniale debba derivare dal prodotto "irregolare" del processo di elaborazione, rende irrilevante il modo utilizzato dall'autore per realizzarla.

Strutturando così la norma, i legislatori hanno cercato di ricomprendervi tutte quelle condotte idonee a modificare il sistema operativo dell'elaboratore. Un'altra conseguenza di questa ricostruzione è che il danno deve necessariamente e direttamente derivare dagli effetti comportati dal risultato della manipolazione. Infatti, nel caso della frode informatica, il requisito dell'effetto della condotta fraudolenta sull'elaborazione dei dati sembrerebbe, al contempo, sia la sostituzione dell'elemento dell'inganno che quello implicito dell'atto di disposizione patrimoniale proprio del reato di truffa[22].

Il legislatore italiano, invece, ha strutturato la norma in termini ambigui, senza includervi l'elemento del risultato irregolare del processo di elaborazione dei dati e quindi anche l'atto di disposizione. Sono stati mantenuti però gli elementi dell'ingiusto profitto e dell'inganno[23]. È evidente come sia stata data priorità al modello della truffa: l'articolo è stato collocato in prossimità dell'art. 640 c.p. e sono stati previsti non solo lo stesso trattamento sanzionatorio ma anche le stesse circostanze aggravanti. Inoltre, l'art. 640 *ter* c.p. è stato strutturato come reato di evento - danno e profitto - a dolo generico[24].

### 1.1. Il bene giuridico oggetto del reato di frode informatica.

Per trattare correttamente il tema dell'oggetto giuridico del reato di frode informatica è necessario, innanzitutto, fare delle considerazioni circa la logica che ha guidato il legislatore nell'inquadrare sistematicamente le figure criminose contro il patrimonio.

Si è spesso ravvisata la tendenza a sacrificare le peculiarità e differenze che caratterizzano le differenti fattispecie a favore della ricerca di un inquadramento unitario dei reati contro il patrimonio e della definizione di categorie generali[25].

---

[21] Secondo PECORELLA, *Diritto penale*, *cit.,* p. 64 e BARTOLI, *op. cit.,* p. 389, i Paesi Europei che hanno optato per questa struttura sono, ad esempio, la Germania, l'Austria e ancora il Portogallo.
[22] Ricostruzione elaborata da PECORELLA, *Diritto penale*, *cit.,* p. 66.
[23] *Ivi.,* p. 64; SCOPINARO, *op. cit.,* p. 44.
[24] *Ivi.*, p. 48.
[25] PALOMBI- PICA, *Diritto penale dell'economia e dell'impresa*, Torino, 1996, p. 552.

Questa tendenza, definita anche come "errore metodologico"[26], che non si verifica solo nel caso del diritto penale contro il patrimonio, ma anche in altri settori[27] ha portato alle stesse conseguenze che si sono presentate in seguito alle classificazioni avvenute in base al bene giuridico tutelato o ancora alle modalità di condotta. Questi criteri guida della classificazione delle norme penali, infatti, accomunano nella stessa categoria fattispecie che risultano essere tutt'altro che assimilabili[28].

Sulla base della collocazione sistematica e della struttura della norma, la dottrina maggioritaria ha rilevato come il bene oggetto dell'art.640 *ter* sia il patrimonio[29]. Infatti, come già rilevato in precedenza, la norma si colloca nell'ambito dei Delitti contro il patrimonio.

Sotto il punto di vista della struttura della norma, emerge che il reato di frode informatica si consuma solo qualora si siano verificati sia il profitto a favore del soggetto agente o di altri che il conseguente danno patrimoniale nei confronti della vittima. Nonostante la norma preveda delle condotte tipiche, limitandone l'applicazione[30], non si tratta di un reato di mera condotta, bensì di evento. Infatti, le due condotte tipizzate dalla disposizione assumono rilevanza penale solo qualora vi sia un nesso eziologico con il "conseguimento di un profitto ingiusto per sé o per altri"[31]. Questa circostanza rende impossibile ritenere valida la concezione per la quale l'art. 640 *ter* c.p. sarebbe preposto alla tutela della riservatezza e al regolare funzionamento dell'operatore[32], essendoci già nel Codice alcune norme poste a tutela di questi beni[33].

La dottrina che ha assistito all'entrata in vigore della legge sui reati informatici si è per molto tempo questionata sull'esistenza di un nuovo bene "informatico"[34], e, in particolare, se fosse individuabile un bene unico la cui tutela fosse posta alla base delle nuove fattispecie penali introdotti con la Legge n. 547 del 93.

---

[26] PICA, *op. cit*., p. 155.
[27] PALOMBI- PICA, *op. cit.,* p. 144 secondi i quali lo sforzo della dottrina a favorire l'esigenza di un'unità sistematica con riguardo alle norme in materia di segreto ha portato a diverse perplessità, ma soprattutto a incongruenze interpretative.
[28] *Ivi*., p. 555.
[29] PICA, *op. cit*., p. 156.
[30] PECORELLA, *Diritto penale*, *cit.,* p. 68.
[31] VITALE, *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime,* in *Arch. pen*., 2015, fasc.1, p. 9.
[32] MASI, *Frodi informatiche e attività bancarie*, in *Riv. pen. econ*, 1995, fasc. 7, p. 430 e nello stesso senso PICA, *op. cit*., p. 157, sostiene che la frode informatica voglia tutelare la libertà negoziale, ossia il diritto di ciascuno di disporre liberamente del proprio patrimonio senza ingerenze.
[33] Il d.lgs 196/2003 in materia di tutela dei dati personali o ancora l'accesso abusivo ad un sistema informatico o telematico *ex* art. 615 ter c.p.
[34] FROSINI, *Informatica, diritto e società*, Milano, 1992, p. 319.

Se da una parte taluni parlavano di "intangibilità informatica", intesa come esigenza di mantenere inalterati i processi di elaborazione dei programmi[35], dall'altra alcuni ritenevano identificabili dei singoli beni giuridici tutelati dalle singole norme[36] e altri ancora identificavano il bene informatico come un bene immateriale con carattere di diritto reale[37].

In realtà, non si può parlare propriamente di nuovi beni giuridici, bensì di nuove modalità di aggressione di beni che già esistono oppure di beni che sono nati con l'evoluzione tecnologica. Un esempio in questo senso può essere il domicilio informatico, che si distingue perfettamente da quello fisico, ma che, come questo, mira alla tutela della persona. Ciò che cambia è il contesto in cui viene realizzata la condotta[38].

Nella concezione del mondo informatico propria degli anni '90, il *computer* veniva concepito come "*longa manus*" del dipendente[39] e non come strumento di accesso al *cyberspace*. Conseguentemente, risultava difficile pensare alla frode informatica come un reato con caratteristiche proprie, identificando quindi il bene giuridico in quello proprio del reato di truffa[40]. Il pensiero successivo agli anni 2000, invece, concepisce il delitto di cui all'art. 640 *ter* c.p. come modellato sulla base del reato di truffa, ma con alcune peculiarità[41].

Si può concludere l'analisi ritenendo che il reato di frode informatica è certamente posto a tutela del patrimonio, ma che proprio in virtù di queste sue caratteristiche singolari la sua forza applicativa si estende a favore della tutela di beni secondari come la riservatezza delle comunicazioni e del regolare funzionamento dei sistemi informatici[42].

---

[35] MILITELLO, *"Nuove esigenze di tutela penale e trattamento elettronico delle informazioni",* in *Riv. trim. pen. econ.*, 1992, p. 373.
[36] SIEBER, La *tutela penale dell'informazione*, in *Riv. trim. pen. econ*., 1992, p. 492.
[37] FROSINI, *op. cit*., p. 65.
[38] PECORELLA, *Diritto penale*, *cit.*, p. 30.
[39] PICA, *op. cit*., p. 157.
[40] *Ibidem.*
[41] In questo senso PECORELLA, *Diritto penale*, *cit.*, p. 60.
[42] ANTOLISEI, *Manuale di diritto penale, Parte speciale*, Milano, 2008, p. 386, in cui si ritiene che dal momento che l'art 640-*ter* è un reato informatico non si può non rilevare che questa stessa norma può anche essere considerata come volta a tutelare, sia pure soltanto indirettamente, il «regolare funzionamento dei sistemi informatici e telematici», nonché «la riservatezza che deve accompagnarne l'impiego». In senso concorde PARODI, *I reati patrimoniali,* in *Diritto penale dell'informatica: Reati della rete e sulla rete*, a cura di PARODI-SELLAROLI, Milano, 2020, p. 104. Nello stesso senso in giurisprudenza Cass. Sez. V, n. 4576/ 2003 consultabile sul sito *https://www.penale.it*. e Cass. Sez II, n. 41013/2018, documento integrale consultato sul sito *https://studiolegaleramelli.it*. in cui in motivazione si legge a p. 4 «Il bene giuridico tutelato dal delitto di frode informatica, non può, dunque, essere iscritto esclusivamente nel perimetro della salvaguardia del patrimonio del danneggiato, come pure la collocazione sistematica lascerebbe presupporre, venendo chiaramente in discorso anche l'esigenza di salvaguardare la regolarità di funzionamento dei sistemi informatici – sempre più capillarmente presenti in tutti i settori importanti della vita economica, sociale, ed istituzionale del Paese – la tutela della riservatezza dei dati, spesso sensibili, ivi gestiti, e, infine, aspetto non trascurabile, la stessa certezza e speditezza del traffico giuridico fondata sui dati gestiti dai diversi sistemi informatici (…)».

## 1.2 Le due modalità di condotta: l'alterazione del funzionamento di un sistema informatico o telematico e l'intervento senza diritto su dati, informazioni o programmi.

La condotta fraudolenta ex art. 640 *ter*, "alterazione del funzionamento di un sistema informatico o telematico" o "intervento senza diritto su dati, informazioni o programmi", è descritta solo apparentemente in termini astratti. Infatti, il legislatore, con l'utilizzo delle espressioni "in qualsiasi modo" e "con qualsiasi modalità" sembra avere l'intenzione di estendere l'ambito applicativo della norma a qualunque tipo di condotta, ma in realtà poi la limita prescrivendo la necessaria alterazione del sistema o ancora di un intervento senza diritto. Questa impostazione è stata criticata in dottrina[43] che ha ravvisato un *deficit* di determinatezza. Segnatamente, si è ritenuto che la norma abbia una pretesa di oggettività, ma che difetti di precisione con riguardo alle caratteristiche che dovrebbe assumere la condotta di "alterazione", rendendola così obsoleta.

Per analizzare compiutamente le condotte incriminate bisogna, innanzitutto, procedere a definire precisamente quale sia l'oggetto materiale della condotta, ossia il "sistema informatico o telematico" da una parte e i "dati, informazioni e programmi" dall'altra.

L'esigenza del legislatore è stata quella di trovare un punto di equilibrio tra la necessità di utilizzare termini tecnici e sintetici per descrivere il fenomeno tecnologico e quella di evitare di ricorrere ad un linguaggio troppo settoriale, che con la rapida evoluzione caratteristica del mondo della tecnologia sarebbero diventati obsoleti[44]. Nonostante gli sforzi profusi però, la frode informatica costituisce, ad oggi, «una fattispecie decisamente problematica, dai tratti molto ambigui e priva di una vera e propria identità tipologica»[45].

Partendo dalla nozione di "sistema informatico o telematico", la Cassazione stessa ha dato una definizione unica: «per sistema informatico o telematico deve intendersi un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione, anche parziale, di tecnologie informatiche, che sono caratterizzate

---

[43] FONDAROLI, *La tutela penale dei beni informatici*, in *Dir. Inform*., 1996, fasc. 6, p. 307. Non sono mancate però visioni contrarie, come quella avanzata da MUCCIARELLI, *Commento all'art. 10 della l. 23/12/1993. n. 547*, in *Leg. pen*., 1996, p. 137, in cui si ritiene che la condotta descritta all'art. 640 *ter* sia più precisa con riguardo alle modalità di aggressione, rispetto alla condotta di "artifici e raggiri" prescritta all'art. 640 c.p.

[44] PECORELLA, *Diritto penale*, *cit.*, p. 69 e PARODI, *op. cit.,* p. 104 in cui si legge che «l'obsolescenza dei processi informatici e telematici è sorprendente: se la norma avesse in qualche modo preso in considerazione la situazione tecnica al momento della sua entrata in vigore sarebbe divenuta inutilizzabile nel volgere di un arco temporale brevissimo. Anche per tale ragione, le indicazioni di massima previste dall'articolo 640 t*er* c.p. sono state in grado di resistere nel tempo, adeguandosi senza particolari difficoltà a scenari di criminalità informatica insospettabili al momento dell'entrata in vigore della legge numero 547 del 1993».

[45] PECORELLA, *Diritto penale*, *cit.*, p. 67; SCOPINARO, *op. cit*., 44; BARTOLI, *op.cit.* p. 392.

– per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»[46].

Importante, con riguardo all'espressione "sistema informatico", è definirne il contenuto. Infatti, guardando la Relazione di accompagnamento al disegno di legge sulla criminalità informatica emerge la volontà di far riferimento «sia a sistemi di scrittura o di automazione d'ufficio ad uso individuale o particolare, sia complessi sistemi di elaborazione dati in grado di fornire servizi e potenza calcolo a migliaia di utenti, sull'intero territorio nazionale ed anche oltre i confini del Paese»[47]. Quindi, rientrano nella nozione non solo i sistemi informatici "semplici", come la carta a microprocessore che si caratterizza per avere un *microcomputer* registrato su "*microchip*"[48], ma anche quelli "complessi", che consistono nell'interazione e interconnessione tra più elaboratori anche situati a notevole distanza[49]. Entrambe queste tipologie sono volte all'elaborazione di dati; il sistema "telematico" svolge invece l'attività di elaborazione e/o trasmissione dei dati elaborati o da elaborare. La scelta del legislatore di inserire l'espressione "sistema telematico" risulta apparentemente superflua perché «un sistema di elaborazione di dati connesso ad una rete di trasmissione di dati», come quella telefonica, è da qualificare prima di tutto come sistema informatico[50]. In realtà questa precisazione è stata inserita per garantire certezza applicativa alla norma.

Ora, è necessario chiarire quale sia la condotta concreta a cui si fa riferimento con l'espressione "l'alterazione del funzionamento di un sistema informatico o telematico".

In un primo tempo ci si chiedeva se questa condotta potesse consistere in una mera alterazione estrinseca, senza impatto sui dati ed esiti del processo di elaborazione, oppure in un'alterazione idonea a produrre le già menzionate conseguenze. Qualora si fosse preferito il primo orientamento, si sarebbe arrivati ad una estensione eccessiva di tutela, potendo applicare la norma anche in caso di condotte caratterizzate da un disvalore tenue o riconducibili ad altre fattispecie. Invece, con il secondo orientamento si sarebbe valorizzata

[46] VITALE, *Brevi riflessioni sul reato di "frode informatica"*, *op.cit*., p. 6 e sul punto si veda Cass., Sez. IV, n. 3067/1999.
[47] Relazione consultabile sul sito *http://legislature.camera.it.*
[48] PECORELLA, *Diritto penale*, *cit.*, p. 72.
[49] *Ibidem* e VITALE, *op. cit*., p. 6.
[50] PECORELLA, *Diritto penale*, *cit.*, p. 73 e nello stesso senso Cass., Sez. VI, n.3067/1999.

una ricostruzione della frode che si incentra sull'inganno realizzato ai danni del *computer*[51]. In giurisprudenza è prevalsa la prima ricostruzione[52] ritenendo che questa condotta di debba concretizzare in un'alterazione "estrinseca" del sistema[53].

La Cassazione, nel 2011[54] e 2013[55], ha specificato, con la prima pronuncia, che «per alterazione deve intendersi ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato (…)», invece con la seconda che «per alterazione del funzionamento di un sistema informatico o telematico deve intendersi (ex art. 640-ter c.p.) ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software: si tratta di un reato a forma libera (…)». Quindi, si può agevolmente affermare che la condotta di riferimento consista in una sostituzione del programma o modifica di questo che porti a un'alterazione delle normali funzionalità[56] dell'elaboratore[57].

La seconda condotta tipizzata dal legislatore è quella di "intervento senza diritto su dati, informazioni o programmi". Il primo elemento che merita menzione, nonché il più problematico, è l'inciso "senza diritto". Infatti, se nel caso dell'alterazione non rileva che la condotta sia stata realizzata da parte di un soggetto autorizzato all'utilizzo del *computer*, in questo caso, invece, la mancanza dell'autorizzazione sembrerebbe essere necessaria. Non può tacersi la presenza anche di chi ha sostenuto che questa seconda condotta rappresenta in realtà una precisazione della prima e non un'alternativa[58]. Questo inciso, potendo voler dire sia totale che parziale assenza di autorizzazione, ha rappresentato una fonte di forte ambiguità.

---

[51] BARTOLI, *op. cit.,* p. 392.
[52] Cass., Sez. V n. 27135/ 2010 per la quale nel caso di apposizione di una seconda scheda all'interno di un impianto di gioco si rientra nell'ambito di applicazione dell'art. 640 *ter* c.p.
[53] PARODI, *op. cit*., p. 106.
[54] Cass., Sez. II n. 249675/ 2011.
[55] Cass., Sez. II, n. 13475/ 2013.
[56] Intese da PECORELLA, *Diritto penale*, *cit.*, p. 82 come "qualsiasi funzione che il computer sia chiamato a svolgere, e non solo quella di elaborazione e trasmissione di dati".
[57] PARODI, *op. cit*., p. 106.
[58] PICA, *op. cit*., p. 144 secondo il quale pur essendovi la disgiuntiva "o" a dividere le due condotte e a postulare un'alternatività, in realtà tra le due non vi sarebbe una separazione concettuale dal momento che sul piano logico l'intervento sui dati o programmi per definizione altera e quindi modifica il funzionamento, l'ordine logico, del computer.

In base a una prima impostazione, l'inciso "senza diritto" avrebbe la funzione di sottolineare la necessità che il comportamento fraudolento avvenga in assenza di una causa di giustificazione, così da escludere l'applicazione dell'art. 51 c.p.[59]. In realtà questa ricostruzione non sembra convincere, soprattutto per il fatto che nel novero dei reati realizzabili contro il patrimonio, l'art. 51 c.p. non è l'unica disposizione che può trovare applicazione. Infatti, se in presenza dei giusti presupposti, anche l'art. 50 c.p. può trovare un ambito di operatività[60].

Inoltre, non sembra esserci coerenza tra l'assenza di questa espressione a caratterizzare le altre disposizioni inserite con la legge n. 547 e il carattere di norma generale che richiama una causa di non punibilità. Se lo stesso inciso fosse stato introdotto anche con riferimento, ad esempio, alla norma sul danneggiamento informatico, si sarebbe potuto sostenere la sua qualifica di pleonasmo. Sostanzialmente, l'inciso, interpretato in questi termini, rimanderebbe alla disciplina prevista nella legge nazionale di ciascuno Stato in materia di causa di non punibilità[61]. A questo punto però, non si riesce a trovare una giustificazione logica sul perché l'inciso non sia stato inserito anche con riferimento alla prima condotta di alterazione ex art. 640 *ter* c.p.

Dalla Relazione alla legge emerge come ciò che inizialmente era stato descritto come "abusivo intervento"[62], nella norma inserita nel Codice è stato poi descritto come "intervento senza diritto". Conseguentemente, l'inciso, in base a questa diversa interpretazione, non svolgerebbe la funzione di rinvio a una causa di non punibilità, ma di specificazione della condotta.

Partendo da questa premessa, due sono le possibili interpretazioni[63]: in base alla prima lettura, l'intervento deve essere commesso da un soggetto che non aveva l'autorizzazione per compierla[64]. Secondo questa linea, sarebbero da escludere i comportamenti abusivi posti in essere da coloro che intrattengono un rapporto diretto e previlegiato con la macchina, come ad esempio il dipendente dell'ente[65]. Se invece si segue un secondo indirizzo, l'inciso

---

[59] Si veda PECORELLA, *Diritto penale*, *cit.*, p. 90, la quale sostiene che l'intervento deve essere posto in essere da una persona non legittimata, quindi in modo arbitrario e ingiustificabile e ANTOLISEI, *op. cit.,* p. 375 in cui si legge che gli interventi rilevanti sono quelli non legittimi.
[60] SCOPINARO, *op. cit*. p 44.
[61] SCOPINARO, *Ivi*., p 45.
[62] Relazione di accompagnamento al disegno di legge n. 2773.
[63] PICA, *op. cit*., p. 146 e PARODI, *op. cit*., p. 107.
[64] PARODI, *Ibidem*. Secondo l'Autore nel caso dell'agente privo, anche in astratto, della possibilità di intervento sul sistema informatico, che realizzi una condotta fraudolenta, è senza dubbio riconducibile alla fattispecie descritta *ex* art. 640 *ter* c.p.
[65] PICA, *op. cit*., p. 147 in cui si legge che uno dei rischi collegati all'inciso è quello di escludere la punibilità dei soggetti "intranei" come il caso dell'operatore bancario.

"senza diritto" viene ricostruito in termini di abuso, facendo quindi rientrare nell'ambito applicativo della norma anche quei soggetti che pur avendo l'autorizzazione ad intervenire sul *computer*, ne abusino, ma escludendola nel caso di soggetti estranei all'ente vittima della frode informatica[66].

Si è notato come questa dicotomia abbia riflessi sull'inclusione o meno della fattispecie di frode informatica nel modello della truffa o in quello del furto. L'ipotesi più classica, e utile in quest'analisi per comprendere questo inciso, è quella del dipendente di banca che fa uso della propria facoltà di accesso ai terminali dell'ufficio per appropriarsi del denaro depositato nei conti correnti dei clienti. Si ritiene che favorire l'interpretazione ampia dell'inciso "senza diritto", quindi idonea a ricomprendere nel suo significato sia il soggetto estraneo che quello dotato di autorizzazione in astratto, ma non quella in concreto, avvicini l'art. 640 *ter* c.p. al modello della truffa. Qualora invece si dovesse prediligere la lettura che ritiene penalmente rilevanti le ipotesi in cui il soggetto agente agisce in assenza di autorizzazione, i casi in cui questa ci sia, ma solo parzialmente, ricadranno nella fattispecie del furto[67]. Nell'ottica della prima opzione, la frode viene percepita come un'ipotesi speciale della truffa[68] facendo leva sul disvalore della condotta di alterazione[69]. Dall'altra parte invece, si trovano coloro che ritengono che, visto l'esito derivato dalla condotta, si tratti di una fattispecie strutturata prendendo come riferimento il modello del furto[70].

Emergono con chiarezza l'ambiguità e i rischi applicativi a cui questa specificazione normativa è idonea a dar luogo, portando la dottrina a caldeggiarne un'immediata modifica.

In generale, la seconda condotta prescritta all'art. 640 *ter* c.p. contempla tutte quelle variazioni che sono volte, anche mediante l'inserimento di informazioni, ad alterare gli esiti delle elaborazioni realizzate dal *computer*[71]. Quindi, vengono ricomprese nella condotta,

---

[66] SCOPINARO, *op. cit.*, p 57.
[67] BARTOLI, *op. cit.,* p. 390.
[68] In questo senso PICA, *op. cit.,* p. 141 e in giurisprudenza emblematica è la Cass., Sez. VI, n. 8755/2009, in cui si afferma che «la fattispecie tracciata ex art. 640-ter c.p. ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il "sistema informatico" di pertinenza alla medesima, attraverso la manipolazione di detta persona».
[69] In senso contrario BARTOLI, *op. cit.,* p. 390 secondo il quale «ogni condotta della frode informatica deve essere diretta in termini più o meno immediati alla manipolazione dei dati e alla interferenza sul programma. Con la conseguenza che se a séguito della condotta di interferenza il software o la sua attività restano inalterati, non si può parlare di vera e propria frode informatica, potendo il fatto eventualmente integrare altre ipotesi di reato».
[70] RECCIA, *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in *Arch. pen*., 2022, fasc. 2, p. 4.
[71] PARODI, *op. cit*., p. 107.

oltre alle manipolazioni di "*input*"[72] - ad esempio quelle volte alla cancellazione di dati o ancora all'introduzione nel processo di dati falsi - e quelle di "*ouput*" - interventi che caratterizzano la fase conclusiva del processo di elaborazione -, anche quelle che hanno ad oggetto un programma oppure delle informazioni[73].

## 2. La fattispecie di utilizzazione indebita di carte di credito o di pagamento ex art 493 *ter* c.p.

La fattispecie di indebito utilizzo di carte di credito o pagamento è stata inizialmente introdotta nell' art. 12 della Legge 5 luglio 1991, n. 197, in materia di "Provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio", sanzionando «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 310 a 1.550 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»[74]. Nel 2007 questa fattispecie è confluita nel D.lgs. n. 231, in particolare all'art. 55, comma nove[75], con lo scopo di dare attuazione alle Direttive: una del 2005/60/CE e l'altra del 2006/70/CE[76] in materia di utilizzo di proventi di reati a scopo di riciclaggio e finanziamento di attività terroristiche.

Ad oggi, a seguito dell'attuazione della delega contenuta all'art. 1, comma ottantacinque, lett. q), della Legge n. 103 del 2017 sulla riserva di Codice penale, oltre ad aver disposto l'abrogazione del summenzionato art. 55, con l'art. 4 del D.lgs. n. 21/2018 il legislatore italiano ha inserito all'art. 493 *ter* c.p.[77] il delitto di indebito utilizzo e

---

[72] PECORELLA, *Diritto penale*, *cit.*, p. 38, le manipolazioni di dati può essere realizzata sia «nella fase iniziale, della raccolta e della introduzione degli *input*, ossia dei dati destinati ad elaborazione (…) che in quella finale, della produzione e emissione in varia forma degli *output*, ossia del risultato della elaborazione».
[73] PECORELLA, *Diritto penale*, *cit.*, p. 90.
[74]Testo articolo 12 della Legge n. 197 del 1991 che può essere consultato sul sito *https://www.softwareantiriciclaggio.it.*
[75] In giurisprudenza, come in Cass, Sez. II, n. 24527/ 2009, è stata sottolineata la continuità normativa tra l'art. 12 e l'art. 55, comma nove.
[76] Cass. Sez. II, n. 11699/2012.
[77] Con Cass. Sez. IV, n. 13492/2020 si è precisato con l'abrogazione dell'art. 55 e la contestuale introduzione dell'art. 493 ter c.p. non si è attuata un*'abolitio criminis*, ma integrerebbe un'ipotesi di continuità normativa

falsificazione di carte di credito o di pagamento nell'ambito dei "Delitti contro la fede pubblica". La scelta di inserire la fattispecie all'interno del Codice è stata giustificata dalla convinzione che il contenuto dell'art. 55 fosse distonico[78] rispetto al testo normativo di riferimento sulla prevenzione al riciclaggio[79].

L'introduzione dell'originario art. 12 con la novella del '91 ha rappresentato la risposta del legislatore alle difficoltà interpretative che erano emerse dall'applicazione della disciplina previgente a nuovi fenomeni dovuti all'avanzamento della tecnologia. Alla fine degli anni '80 si era assistito all'emersione di una nuova forma di frode, che ha trovato la propria origine nella diffusione dei distributori automatici di banconote[80], consistente sia nel prelievo di denaro avvalendosi di carte altrui o falsificate che nel prelievo, da parte del titolare della carta, di una somma che superasse il saldo disponibile sul conto[81]. La possibilità poi introdotta a favore dei titolari di queste carte di poter effettuare pagamenti con il *point of sale* (P.o.s), ossia effettuare acquisiti nei confronti degli esercizi convenzionati, ha portato ad ampliare le possibilità di commissione di abuso delle carte magnetiche[82].

A differenza delle carte tradizionali, come ad esempio quelle di credito, la carta magnetica, anche conosciuta come carta "di debito", è idonea di per sé a dare inizio a un processo di elaborazione di dati che comporta contestualmente un profitto a favore del soggetto agente, ed un danno in capo al titolare della carta[83].

Come era avvenuto per gli analoghi fatti di frode informatica prima dell'introduzione della novella del '93, il dubbio interpretativo aveva riguardato la possibilità di ricorrere all'applicazione a questi nuovi fatti del reato *ex* art. 640 c.p. o di quello *ex* art. 625 c.p. Se da una parte risultava facilmente applicabile il reato di truffa con riguardo all'abuso di carte tradizionali da parte di terzi ravvisando l'induzione in errore dell'esercente convenzionato,

---

per la quale è possibile far riferimento agli orientamenti dottrinali e giurisprudenziali che si sono succeduti con riguardo all'art. 12 d.l del 91 e art. 55 d.lgs del 2007.

[78] In dottrina, in particolare CORRADINO, *La tutela penale del sistema dei pagamenti,* in *Banca, borsa, tit. cred.* 2001, fasc. 2, p. 121, si è parlato di norma "intrusa".

[79] Nello schema di Decreto legislativo recante le "Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103", consultabile sul sito https://www.consigliolegale.com, p. 5 si legge con riferimenti all'art. 55, comma cinque che «Si è in presenza di una disposizione del tutto estranea al testo normativo di riferimento dedicato alla prevenzione del riciclaggio e, pertanto, adeguatamente inseribile nel codice penale».

[80] PECORELLA, *L'abuso dei distributori automatici di banconote*, in *Riv. it. dir. proc. pen*., 1990, fasc. 2, p. 573, servizio che nel nostro paese è diventato operativo nel 1983 e consente ai titolari che sono in possesso di una carta magnetica abilitata e del relativo *personal identification numbe*r (P.i.n) di poter prelevare contante.

[81] PECORELLA, *Diritto penale, cit.,* p. 46.

[82] PECORELLA, *Ivi.,* p. 47.

[83] SCOPINARO, *op. cit.*, p 67 e 68; Detto in altre parole si veda PECORELLA, *Ibidem*., «la carta magnetica di prelievo (…) comporta l'immediato addebito sul conto corrente del titolare delle spese e dei prelievi effettuati».

dall'altra questo elemento veniva a mancare con riguardo alle carte magnetiche. Infatti, in questa ipotesi l'unico rapporto ravvisabile era quello tra il soggetto agente e una macchina[84].

Anche con riguardo all'applicabilità della fattispecie del furto sono emerse alcune perplessità. In particolare, questa poteva risultare applicabile, in base all'assimilazione tra la carta magnetica e la chiave di accesso a una cassaforte[85], nel caso di prelievo di denaro da un distributore automatico mentre con riguardo all'ipotesi di utilizzo abusivo della carta come metodo di pagamento con P.o.s, questa ricostruzione non avrebbe trovato senso alcuno.

Un altro problema si era verificato con riguardo alle condotte di contraffazione e alterazione delle carte magnetiche: queste, infatti, vista l'invisibilità delle informazioni registrate sulla banda magnetica che le caratterizza, non possono rientrare nella nozione di "documento" accolta da giurisprudenza e dottrina, portando all'inapplicabilità delle norme sulle falsità documentali[86]. Questa questione non si poneva invece con riguardo alle carte tradizionali, per le quali l'abuso del finto titolare avrebbe comportato necessariamente la realizzazione del reato *ex* art. 485 c.p. in materia di uso di scrittura privata falsa[87], dovendo l'agente apporre una firma falsa sull'ordine di pagamento.

L'art. 12 è un reato a dolo specifico che consiste nella volontà e consapevolezza di utilizzare indebitamente, di falsificare o alterare la carta, o ancora, di possederla, cederla, acquisirla. La disposizione punisce tre diverse condotte con il medesimo trattamento sanzionatorio. La prima parte della norma si incentra sull'utilizzazione indebita da parte di colui che non è titolare di «carte di credito o di pagamento[88], ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi», che può essere definito come il fatto principale[89]. Nella seconda parte del dettato normativo è evidente la scelta del legislatore di anticipare la soglia di punibilità

---

[84] PECORELLA, *Diritto penale, cit.,* p. 48.

[85] Come nel caso della Cass, Sez. II n. 1162/1989 in cui si riconobbe la configurabilità del furto aggravato nel caso di appropriazione di banconote prelevate da uno sportello automatico mediante una carta "Bancomat". A favore di questa ricostruzione vedi anche MUCCIARELLI, *op. cit.,* p. 373 secondo il quale la carta magnetica duplicata o falsata equivarrebbe alla chiave duplicata o falsata che verrebbe utilizzata per aprire una cassaforte e prelevare denaro, potendo quindi applicarsi l'art. 624 e 625, n. 2 c.p.

[86] PECORELLA, *Diritto penale, cit.,* p. 49.

[87] SCOPINARO, *op. cit.*, p 68 e 69.

[88] PECORELLA, *Diritto penale, cit.,* p. 56, la norma ricomprende non solo le carte di credito, ma anche quelle di debito e le carte - assegni. La ricomprensione delle carte magnetiche emerge dall'espressione «ogni altro documento analogo che abiliti all'acquisto di beni o alla prestazione di servizi». Inoltre, con l'espressione «altri documenti con analoga funzione» si voleva ricomprendere ogni supporto con la medesima utilità economica e questo ha portato la giurisprudenza a farvi rientrare, ad esempio, la "viacard", ossia la tessera per il pagamento del pedaggio nelle autostrade, nella Cass., Sez. II, n. 36295/2005 o, ancora le S.U. nel 2001, n. 22902 hanno affermato la ricomprensione della *smart card* per noleggiare i *dvd.*

[89] PICA, *op. cit*., p. 163.

sanzionando condotte prodromiche all'uso stesso [90]: si punisce colui che «falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo (…)». Infine, si puniscono condotte collegate alla circolazione, ossia il possesso, la cessione o l'acquisizione di «tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento[91] prodotti con essi».

Se per la condotta di utilizzazione il legislatore specifica la qualità soggettiva di "non titolare", non potendo quindi il reato essere realizzato dal proprietario della carta, ciò non avviene per quanto riguarda le condotte di falsificazione e alterazione. La prima si sostanzia nella realizzazione di una carta di pagamento simile a quella originale, mentre la seconda consiste in qualsiasi variazione apportata ai dati della carta come, ad esempio, la data di scadenza o il nominativo del titolare[92]. Per quanto riguarda la "provenienza illecita", inserita dal legislatore come presupposto delle condotte di possesso, acquisizione e cessione, alcuni ritengono che tale illeceità possa essere non solo di natura penale, ma anche civile e amministrativa[93]. Infine, le condotte di acquisizione e cessione fanno riferimento a qualsiasi tipo di trasferimento, oneroso o gratuito, della carta[94].

L'analisi effettuata sino a questo punto può essere applicata anche al nuovo art. 493 *ter* c.p. trattandosi di un'ipotesi di continuità normativa e non avendo subito mutazioni con riguardo alla sua formulazione[95].

Il predetto reato ha ad oggetto la tutela non solo del patrimonio individuale, ma anche della fede pubblica[96] e, per la sua natura di reato di pericolo presunto, si consuma anche solo con il mero possesso della carta di pagamento, a prescindere dal conseguimento effettivo del profitto ingiusto[97].

---

[90] PECORELLA, *L'abuso dei distributori automatici,* cit., p. 260, in cui l'Autrice sottolinea che la scelta del legislatore di circoscrivere la fattispecie alla sola ipotesi in cui oggetto di abuso sia una carta autentica deriva dalla volontà di prevedere nella stessa disposizione la punibilità del mero possesso di carte o documenti di provenienza illecita o comunque falsificati o alterati così da anticipare la soglia di punibilità delle condotte ad un momento anteriore e prodromico rispetto a quello dell'utilizzazione.

[91] Espressione con cui si fa riferimento ai cosiddetti *voucher*, ossia documenti sottoscritti dal cliente nell'atto di acquisto con carta di credito consentendo al venditore di ricevere il pagamento dei beni acquistati "a credito".

[92] PICA, *op. cit*., p. 164.

[93] PECORELLA, *Il nuovo diritto penale delle carte di pagamento*, in *Riv. it. dir. proc. pen.*, 1993, fasc. 1, p. 271.

[94] PICA, *op. cit*., p. 165.

[95] Cass. Sez. IV, n. 13492/2020.

[96] Cass., Sez. V, n. 18680/2021 in cui è stata affermata la plurioffensività di questa fattispecie.

[97] Cass., Sez. V, n. 17923/ 2018 in cui la Cassazione ha ritenuto il reato consumato affermando che la accertata utilizzazione della carta "bancomat", di illecita provenienza, di chi non abbia il codice Pin, realizzata mediante la digitazione casuale di sequenze numeriche presso uno sportello di prelievo automatico di denaro, doveva considerarsi tale da esaurire l'attitudine lesiva dei beni giuridici dell'ordine pubblico economico e della fede pubblica, sufficiente a integrare la fattispecie consumata di utilizzazione indebita di carta abilitante al prelievo di denaro contante.

Per quanto riguarda i rapporti tra l'art. 493 *ter* c.p. e l'art. 640 *ter* c.p., la Cassazione è pacifica nel ritenere che colui che, in assenza di frode, utilizzi indebitamente il codice e una tessera *Bancomat* per effettuare prelievi di denaro realizza il reato di utilizzo indebito di carte di pagamento[98].

Invece, si è registrato[99] un contrasto giurisprudenziale con riguardo alla qualificazione giuridica dell'utilizzo indebito di supporti magnetici clonati: a chi ritiene configurabile il reato di frode informatica si contrappone chi avvalora la ricostruzione in termini di utilizzo indebito di carte di pagamento[100].

Un primo filone di giurisprudenza che ha ritenuto sussistente l'utilizzazione fraudolenta del sistema informatico, consistente nella penetrazione senza diritto nel sistema bancario mediante una carta falsata e la captazione del codice d'accesso, affermando che ciò costituisce «un presupposto assorbente rispetto alla generica indebita utilizzazione di una carta di credito, iscritta, come ratio, nel novero di misure destinate al controllo dei flussi finanziari, in funzione di prevenzione del riciclaggio»[101]. Sempre secondo la Corte, questa ricostruzione sarebbe funzionale all'applicazione del principio di specialità volto a garantire il rispetto dei tradizionali criteri interpretativi delle disposizioni[102].

Dall'altra parte, però, la stessa Corte ha sottolineato che «l'assorbimento del reato di cui all'art. 640 ter c.p. nella previsione di cui all'art. 55 comma 9 cit. attiene alla condotta di 'indebita utilizzazione' e non a quella di falsificazione o alterazione di carta di credito, autonomamente prevista da tale ultima norma, la quale concorre quindi con il delitto di frode informatica»[103]. Conseguentemente, nel solo caso di colui che abbia ottenuto i dati relativi a una carta e li abbia utilizzati indebitamente come strumento di pagamento per trarne un profitto proprio, sembrerebbe potersi verificare un concorso apparente delle due norme[104].

Da quanto esposto emerge chiaramente come il dibattito giurisprudenziale attorno al rapporto tra il reato di frode informatica e quello di utilizzazione indebita di carte di pagamento non sia ancora arrivato a una soluzione univoca e che non possa venire facilmente in ausilio all'interprete[105].

---

[98] Cass., Sez. II, n. 50395/ 2019 e dello stesso anno la n. 30480.
[99] La stessa Corte in Cass., Sez. II, n. 8913/ 2017, ha affermato che sul punto non può non rilevarsi l'esistenza di un contrasto giurisprudenziale.
[100] Così Cass., Sez. II, n. 41777/ 2015.
[101] Cass., Sez. II, n. 17748/ 2011.
[102] FALDUTI, *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative*, in *Giur. Pen*., 2017, fasc. 2, p. 3.
[103] Cass., Sez. II, n. 46981/ 2016.
[104] FALDUTI, *op.cit.,* p. 3.
[105] FALDUTI, *Ivi.,* p. 1.

### 3. La nuova variante del "*Phishing*".

Si è visto come l'evoluzione della tecnologia e lo sfruttamento dell'immaterialità del *cyber* spazio abbiano agevolato la diffusione nel panorama criminale di fattispecie, come il *phishing* o l'abuso dell'identità virtuale, che posso essere ricondotte nella categoria dei cosiddetti *"Identity crimes"*[106]. L'elemento che accomuna tutti questi comportamenti è il fatto che il soggetto agente inizialmente si limiti alla raccolta di dati personali o codici di accesso di un soggetto ignaro, sostituendosi a quest'ultimo, per farne uso in seguito compiendo attività illecite mantenendo l'anonimato. Le tecniche mediante le quali i *cyber*-criminali carpiscono i dati personali al fine di duplicare o creare una nuova identità, sono le più disparate, quali, ad esempio, il *social engineering* sulla rete che spesso caratterizza la pratica del *phishing*, l'*hijacking*[107], o, ancora, il *trashing* e l'*hachering*[108].

La diffusione di questa tipologia di crimini ha evidenziato nuovamente il difficile adeguamento del diritto vigente[109] a questi fatti costituenti un nuovo modello "ibrido" di *cybercrimes*, che si presentano in concreto come una combinazione tra crimini tradizionali e nuove modalità di aggressione ai beni giuridici[110].

Il fenomeno del *phishing*[111] può essere definito come «una tecnica di *social engineering*[112], in quanto è una metodologia di comportamento sociale indirizzate a carpire

---

[106] Espressione che viene utilizzata in FLICK, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. inform*, 2008, fasc. 4-5, p. 526, per indicare quelle aggressioni che hanno ad oggetto l'identità digitale altrui, dovendo farvi rientrare tutte quelle informazioni online concernenti una persona, ente ecc.

[107] Secondo CAJANI, *Profili penali del Phishing*, in *Cass. pen*., 2007, fasc. 6, p. 2295, consiste nel dirottamento del browser e tendenzialmente ha come fine ultimo la volontà di indirizzare il navigatore su un sito diverso rispetto a quello digitato sulla barra di ricerca.

[108] SCHIPANI, *Furto d'identità, frodi informatiche e phishing*, in *La criminalità informatica*, a cura di GALDIERI, in *Riv. elettr. dir. econ. man*., 2013, fasc. 3, p. 46, definisce il *trashing* come sottrazione dei dati necessari attraverso documenti smarriti o addirittura rinvenuti nella spazzatura e l'*hackering* come intervento forzato su un sistema informatico altrui.

[109] La novella del 93 in materia di criminalità informatica ha rappresentato una svolta nella lotta contro questo fenomeno. Prima, infatti, le nuove esigenze di tutela venivano fronteggiate mediante interventi frammentari o con tentativi interpretativi da parte della giurisprudenza. Per un approfondimento a riguardo si veda PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di internet*, a cura di PICOTTI, Padova, 2005, p. 30 o ancora ID, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. int*, 2005, fasc. 2, p. 189.

[110] FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir e proc. pen*., fasc. 2 – 3, 2007, p. 2.

[111] SCHIPANI, *op. cit.*, p. 46, «il termine è stato coniato parafrasando il verbo inglese "*to fish*", che significa pescare. Tramite questa tecnica, infatti, i cybercriminali cercano appunto di "pescare" i dati personali di utenti della rete per successivamente utilizzarli per le più svariate attività delittuose».

[112] SARZANA DI SANT'IPPOLITO, *Informatica, Internet e diritto penale*, Torino, 2010, p. 378 chiarisce che «per ingegneria sociale si intende l'attività diretta ad ottenere informazioni direttamente dalla vittima o da una persona a lei vicina, mediante l'assunzione di una fase identità. (…) Il vero *social engineer*, prima di mettere in atto il crimine, "studia" le vittime, usando varie tecniche per raccogliere il massimo delle informazioni sui sistemi di comunicazione adoperati e sulla posta elettronica».

informazioni personali oppure abitudini e stili di vita»[113]. Una definizione che si pone sulla stessa linea è stata fornita nel 2011 dalla Corte di Cassazione, in base alla quale «il *phishing* è quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici ed *malware*) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (*user e password*) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati»[114].

Quindi, il *phishing* costituirebbe una pratica volta a carpire dati e informazioni sensibili[115] mediante l'utilizzo delle comunicazioni elettroniche, come ad esempio, le *e-mail*[116]. Generalmente, anche se si tratta di un fenomeno in continua evoluzione[117], il *modus operandi* del *phisher* consiste nell'invio, fingendosi un ente o un'istituzione reale, di messaggi di posta elettronica casuali contenenti un testo ingannevole[118] a un numero indefinito di utenti[119]. Tendenzialmente, questi messaggi hanno il fine ultimo di allarmare l'utente: spesso, infatti, indicano un tentativo di intrusione sul conto, problemi del *server* o, più semplicemente, contengono un avviso di aggiornamento del profilo[120]. Il senso di preoccupazione e la situazione di urgenza che viene percepita dall'utente lo inducono a cliccare il *link* presente nel messaggio. Il collegamento ipertestuale ha la funzione di indirizzare il soggetto ad una pagina *web* non autentica[121] per consentirgli di inserire i dati di accesso alle aree riservate. Una volta avvenuto l'impossessamento dei dati, il soggetto

---

[113] FLOR, *Ivi.*, p. 3.
[114] Cass., Sez. II, n. 9891/2011.
[115] Come, ad esempio, le credenziali di autenticazione per accedere a servizi finanziari online, numeri di carte di pagamento, Id e password per l'accesso diretto alle applicazioni di home banking o ancora gli estremi dei documenti d'identità.
[116] Pratica che prende il nome di "*spamming"* che consiste nell'invio di messaggi, maggiormente di posta elettronica, indesiderati, come specificato da SCHIPANI, *op. cit.*, p. 47. A riguardo si veda anche DESTITO – DEZZANI – SANTORIELLO, in *Il diritto penale delle nuove tecnologie*, Milano, 2007, p. 69 e CAJANI, *op. cit*., p. 2294.
[117] L'evoluzione e il perfezionamento delle modalità di attacco hanno portato alla nascita di nuove tipologie di *phishing attacks*, come quelli che si sostanziano nell'auto installazione di software (Trojan o *maleware*) o, ancora i *phishing Voip*. Per comprendere meglio la dimensione del fenomeno si vedano i rapporti elaborati *dall'Anti- Phishing Working Group* (APWG) sul sito http://www.antiphishing.org/.
[118] SARZANA DI SANT'IPPOLITO, *op. cit*., p. 378 parla di "messaggio- trappola" inviato a un numero elevato di utenti aumentando così le probabilità di raggiungere l'utente che detiene il proprio conto presso la banca o l'istituto di credito indicato come emittente del messaggio.
[119] Da qui deriva il nome "pesca con l'amo", utilizzato da DESTITO – DEZZANI – SANTORIELLO, *op. cit*., p. 72, proprio perché il messaggio viene inviato casualmente senza che il *phisher* abbia alcuna informazione sul tipo di banca utilizzata dal destinatario della *mail*. Detto in altri termini «il mittente del messaggio lancia un'esca senza sapere chi abboccherà».
[120] RECCIA, *op.cit*., p. 6.
[121] Questa è la tecnica del "*phraming*" che consiste nel reindirizzare il traffico da un *website* ad un altro falso, come specificato da SARZANA DI SANT'IPPOLITO, *Ibidem*. Più nello specifico si veda AMATO MANGIAMELI – SARACENI, in *Reati informatici: elementi di teoria generale e principali figure criminose*, Torino, 2015, p. 17.

agente li utilizza per accedere lui stesso, assumendo l'identità virtuale della vittima, ai servizi *online*[122] e compiere attività illecite come il trasferimento di somme di denaro.

All'assenza nell'ordinamento italiano di una disciplina specifica volta a sanzionare il *phishing*, si affianca la circostanza per la quale quest'ultimo è un fenomeno a più facce, che ne rende estremamente difficoltoso l'inquadramento giuridico.

Un punto di partenza può essere la divisione sistematica della fattispecie in tre fasi: in una prima fase si invia il messaggio di posta elettronica con il *link* alla pagina non autentica; la seconda fase, invece, consiste nella "pesca" dei dati riservati; nella terza, infine, il soggetto agente utilizza le informazioni carpite per accedere abusivamente al servizio *online* o utilizza indebitamente le carte di pagamento[123].

Altra parte della dottrina[124] distingue, invece, sei fasi: i) il *planning,* in cui il *phisher* individua e "studia" la vittima e come porre in essere il proprio approccio; ii) il *set up,* in cui l'autore prepara gli strumenti per realizzare la condotta; iii) una volta realizzate le due fasi preparatorie, il *phisher* pone in essere l'attacco vero e proprio (*attack*); iv) il risultato di quest'ultima fase è la cosiddetta *collection* dei dati e delle informazioni personali; v) ottenute queste, il *reo* procederà a compiere le più disparate attività fraudolente (*fraud*); vi) l'ultima fase consiste nel *post attack* ossia eliminare le possibili tracce a favore dell'anonimato. Ciò che salta subito all'occhio è il fatto che i *phishing attacks* possono essere facilmente scomposti e, non essendo presente nell'ordinamento italiano una normativa *ad hoc,* le singole condotte possono essere assoggettate a diverse diposizioni penali, quali gli artt. 494 (sostituzione di persona), 615 *ter* (accesso abusivo in un sistema telematico o informatico), 640 *ter* (frode informatica) c.p., l'art. 615 *quinquies* (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico) c.p., o altre ancora come l'art. 167 del D.lgs. 196/ 2003 (trattamento illecito di dati)[125].

Partendo dall'art. 494 c.p., questo potrebbe trovare applicazione nell'attività di *deceptive phishing* in cui si concretizza la fase di "pesca" delle vittime. In particolare, la condotta di invio di messaggi di posta apparentemente provenienti da mittenti "reali"

[122] Secondo FLOR, *op. cit*., p. 3, i due obbiettivi che caratterizzano i *phishing attacks* sono: portare l'utente a fornire dati o informazioni personali e, in secondo luogo, utilizzare quest'ultimi per accedere ai servizi *online*, assumendo l'identità del reale titolare.
[123] FLOR, *Ivi.,* p. 4.
[124] SCHIPANI, *op. cit.*, p. 49.
[125] SCHIPANI, *Ibidem.*

potrebbe integrare le condotte tassativamente previste dal delitto *de quo*[126] solo qualora venga fatto uso degli estremi identificativi di un mittente reale, appropriandosi quindi di un altro nome[127]. La Cassazione, prima nel 2007[128] e poi nel 2011[129], ha affermato che «integra il reato di sostituzione di persona, di cui all'art. 494 c.p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet, nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese». Preme sottolineare che ciò vale nei casi in cui l'identità della persona fisica assunta dal soggetto agente sia determinata.

Qualora invece questa determinatezza non ci sia, come quando la "persona sostituita" risulti essere un ente, una società o un'istituzione, sorgono importanti problemi applicativi della norma[130]. Infatti, la *mail* che ripropone i loghi e i siti degli enti bancari, ad esempio, non ha la stessa valenza di quando il *phisher* utilizza gli estremi identificativi di un mittente "persona fisica"[131] e, pertanto, non è possibile parlare di «sostituzione della propria all'altrui persona»[132].

Inoltre, l'azione realizzata dal *phisher* è quella di utilizzare i dati personali, ossia le credenziali di autenticazione della sua vittima per l'accesso ai servizi *online* o alle aree private del sito. Di conseguenza, non può dirsi integrato l'elemento oggettivo dell'art. 494 c.p., non potendo questa condotta essere assimilata a quella tipizzata dalla norma nell'attribuzione di falso nome, stato o qualità a cui la legge attribuisce effetti giuridici[133].

Un ultimo limite all'applicazione dell'art. 494 c.p. deriva dall'evento consumativo del reato, l'induzione di taluno in errore. Nel caso esaminato questo elemento non risulta

---

[126] Art. 494 c.p «(…) sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici (…)».
[127] FLOR, *op. cit*., p. 5.
[128] Cass., Sez. V n. 46674/ 2007 in cui la Corte afferma che «oggetto della tutela penale, in relazione al delitto preveduto nell'art. 494 c.p., è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome».
[129] Cass., Sez. III n. 12479/ 2011.
[130] RECCIA, *op. cit*., p. 7.
[131] FLOR, *op. cit*., p. 6.
[132] SCHIPANI, *op. cit.*, p. 50; *Contra* Trib. Milano 2011, Pres. Pellegrino, «risponde dei delitti di sostituzione di persona (art. 494 c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615 *ter* c.p.) e truffa (art. 640 c.p.) chi, avvalendosi delle tecniche del c.d. *phishing*, mediante artifici e raggiri realizzati attraverso l'invio di false *e-mail* e la creazione di false pagine *web* in tutto simili a quelle di primari Istituti di Credito, dopo aver indotto in errore l'utente ed essersi fatto rivelare le credenziali di accesso, si introduca nel servizio di *home banking* della vittima per effettuare operazioni di prelievo o bonifico on line non autorizzate». In cui si afferma l'applicabilità dell'art. 494 c.p. nonostante la persona sostituita risulti indeterminata.
[133] FLOR, *op. cit*., p. 6.

essere compatibile con «l'esecuzione automatizzata di richieste inoltrate ai sistemi informatici»[134]. Infatti, l'inserimento da parte del *phisher* delle credenziali appartenenti ad altro soggetto nel sistema informatico non comporta un'induzione in errore di quest'ultimo, il quale, dalla sua, esegue fedelmente i comandi impartiti dalla persona fisica che per esso risulta corrispondere all'identità virtuale utilizzata[135].

Quanto all'art. 615 *ter* c.p., questo è stato inserito nei delitti contro l'inviolabilità del domicilio riprendendo la struttura dell'art. 614 c.p. (violazione di domicilio). Il bene giuridico che viene tutelato dalla disposizione è rappresentato dalla "riservatezza informatica", intesa come «interesse esclusivo di godere, disporre e controllare le informazioni, procedimenti, sistemi e "spazi" informatizzati e le relative utilità»[136].

La norma, nel sanzionare l'accesso non autorizzato ad un sistema informatico o telematico protetto da misure di sicurezza, può avere un margine applicativo nella fase in cui il soggetto agente usa indebitamente le credenziali carpite in precedenza per accedere in via abusiva ad aree informatiche riservate. Il punto cruciale che caratterizza questa fattispecie è l'esistenza di un diritto del titolare di escludere l'accesso indesiderato di terzi (*jus excludendi alios*) che si manifesta nella predisposizione di misure di sicurezza. Non ci sono dubbi nel ritenere, in virtù della loro funzione protettiva, che siano tali anche i codici utente, i PIN e le *password.*

Ai fini della consumazione è sufficiente la sola violazione di detto diritto, non essendo richiesta, ad esempio, la concreta esecuzione di operazioni bancarie o finanziarie[137]. La Suprema Corte ha poi affermato la possibilità di concorso[138] tra questa fattispecie e l'art. 640 *ter* c.p., in virtù della diversità dei loro presupposti giuridici[139]. La Corte, nel 2020[140], ha ribadito come nel caso del reato di accesso abusivo a sistema informatico il bene giuridico tutelato sia il "domicilio informatico", inteso come *jus excludendi alios,* mentre nel caso della frode informatica si «sanziona l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto»[141]. Di conseguenza, nel momento in cui il soggetto agente oltre ad accedere abusivamente al sistema utilizzando l'*account* riservato alla vittima,

---

[134] SCHIPANI, *op. cit.*, p. 51.
[135] FLOR, *op. cit*., p. 6.
[136] FLOR, *Ivi.,* p. 18.
[137] FLOR, *Ivi.,* p. 20.
[138] Cass. Sez. V, n. 1727/2008; confermato da Cass., Sez. II n. 9891/2011; Cass., Sez. V, n. 26604/2019; Cass. Sez. V, n. 17306/2020.
[139] Cass., Sez. V n. 2672/2004 in cui ha affermato che le differenze «si rilevano dalla diversità dei beni giuridici tutelati, dall'elemento soggettivo e dalla previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi di sistemi protetti, caratteristica che non ricorre nel reato di frode informatica».
[140] Cass., Sez. V, n. 17306/2020.
[141] Cass., Sez. V, n. 17306/2020.

procede a manipolare i dati in esso contenuti sarà perseguibile sia ai sensi dell'art. 615 *bis* c.p. che dell'art. 640 *ter* c.p. Diversamente, come affermato nella sentenza n. 26604/2019, in queste ipotesi, visto il duplice danno subito dalla vittima, sarebbe riduttivo ricondurre l'azione criminosa ad un'unica fattispecie di reato[142].

Alla luce della scarsa applicazione dell'art. 494 c.p., il legislatore ha cercato di fronteggiare il fenomeno del *phishing*, non solo con l'art. 640 *ter* c.p., ma anche con l'introduzione all' art. 640 *ter* c.p. nel 2013, di un terzo comma che dispone la pena della reclusione «da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti».

Come già anticipato, il reato di frode informatica trova il suo parente più prossimo in quello di truffa ex art. 640 c.p. In entrambi i reati l'evento è rappresentato dall'ingiusto profitto con l'altrui danno, l'elemento distintivo si sostanzia nella condotta fraudolenta. Infatti, nella frode questa si concretizza in un'alterazione del sistema informatico o in un intervento senza diritto su dati e informazioni[143], mentre nella truffa, il disvalore si incentra nell'induzione in errore di una persona fisica mediante artifici e raggiri. Conseguentemente, la condotta che caratterizza la frode impatta non tanto sulla libertà di autodeterminazione della vittima come nella truffa, ma bensì sul corretto e regolare funzionamento del sistema informatico[144]. Le due fattispecie condividono, inoltre, il trattamento sanzionatorio e le aggravanti.

La fattispecie di frode sconta la convinzione del legislatore di poter ricomprendere ogni tipo di truffa realizzata mediante la tecnologia. In realtà, l'art. 640 *ter* c.p., per quanto riprenda degli elementi propri della truffa comune, se ne distingue con riguardo al rapporto interpersonale con la vittima[145]. A riguardo la giurisprudenza fronteggia il problema sostanzialmente senza porselo[146] e sono proprio queste incertezze a spiegare il motivo per

---

[142] Cass., Sez. V, n. 26604/2019.

[143] FLOR, *op.cit*., p. 7, condotte "fraudolente" sono viste come immediatamente causative del duplice evento.

[144] PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, a cura di PICOTTI, Padova, 2005, p. 55 e FLOR, *op.cit*., p. 8 in cui si legge che appunto l'oggettività giuridica non è costituita solo dal patrimonio, ma anche dall'affidabilità che deve poter avere il soggetto passivo nell'utilizzo delle tecnologie informatiche rispetto ad interventi manipolativi, fraudolenti o abusivi.

[145] Sempre FLOR, *Ibidem*., con riguardo all'art. 640 ter c.p., afferma che in quest'ultima fattispecie rimane certamente un rapporto di cooperazione artificiosa con la vittima, titolare o fruitore del sistema, ma in tal caso la sua volontà è viziata implicitamente o indirettamente dalla causazione di un risultato irregolare, alterato o manipolato delle procedure di trattamento automatizzato, da esso predisposte o utilizzate, che sono direttamente attivate dall' agente.

[146] A titolo di esempio, la sentenza del Trib. Napoli., Sez.VI, n.205/2020, ha evidenziato che: «L'art 640 *ter* c.p. sanziona chi, 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. In tal

cui il nuovo fenomeno del *phishing* è stato ricondotto, in dottrina[147], una volta nell'art. 640 c.p. e un'altra nell'art. 640 *ter* c.p. Ad oggi, la giurisprudenza di legittimità[148] sembra però essere più orientata verso l'applicabilità dell'art. 640 *ter* c.p., in particolare, nei casi in cui il *phisher* utilizzi i dati riservati in suo possesso per intervenire telematicamente senza diritto sui dati, programmi e informazioni della vittima, apportando delle modifiche ai dati concernenti le operazioni bancarie o finanziarie o direttamente al conto corrente, procurandosi in questo modo un ingiusto profitto[149].

Come già accennato, è stato anche affermato il possibile concorso formale con l'art. 615 *ter* c.p. qualora le operazioni attuate dal *phisher* nella fase di utilizzo dei dati, seguano un accesso abusivo[150].

Si può concludere quest'analisi ritenendo che l'unica risposta data dal legislatore ai *phishing attacks* sia stata, nel concreto, l'introduzione dell'aggravante di cui al comma 3 dell'art. 640 *ter* c.p. Si tratta di una scelta ritenuta inadeguata: sarebbe stato forse più efficace prevedere un'autonoma e distinta fattispecie di reato che facesse riferimento, con riguardo

---

modo si vuole tutelare il patrimonio individuale, ma più specificatamente il regolare funzionamento dei sistemi informatici e la riservatezza dei dati ivi contenuti. Per la configurabilità del reato in questione, a differenza di quanto previsto per il reato di cui all'art 640 c.p., non è richiesta l'induzione in errore della vittima, in quanto l'attività fraudolenta investe il sistema informatico della stessa e consiste nell'alterazione, comunque realizzata, del sistema informatico e dell'intervento, senza averne diritto, con qualsiasi modalità, su dati, informazioni, programmi di un sistema informatico».

[147] BARTOLI, *op. cit*., p. 395 ha affermato che parte della giurisprudenza di merito, ritenendo che le fasi di inganno e di utilizzo dei dati carpiti siano congiunte, ha concluso nel senso della configurazione della truffa in concorso con altri reati. In tal senso Trib. Monza 2009 in *Riv. pen*., 2010, p. 1300. Sempre l'Autore, tuttavia, ritiene che queste due fasi siano decisamente slegate, ritenendo quindi più consona la riconduzione della prima fase nel reato di sostituzione di persona e la seconda in quello della frode informatica. Ancora, FLOR, *op.cit*., p. 9- 12 ha affermato l'assenza di dubbi in merito alla corrispondenza agli "artifizi e raggiri" previsti all'. art. 640 c.p. del contenuto del messaggio di posta elettronica, con una determinata struttura grafica, contenente il *link* di indirizzamento alla pagina *web* non autentica. Infatti, è pacifico che questi elementi creino una falsa rappresentazione della realtà, inducendo il destinatario in errore. Tuttavia, un limite applicativo è stato individuato nel requisito implicito della disposizione patrimoniale, espressivo della necessaria cooperazione della vittima: la falsa rappresentazione della realtà e l'induzione in errore possono riguardare solo una "persona fisica" e non un sistema informatico. Ciò ha portato all'inapplicabilità dell'art. 640 c.p. nei casi in cui il *phisher*, ottenuti i dati riservati, li utilizzi per accedere egli stesso abusivamente del sistema per eseguire direttamente le operazioni di suo interesse.

[148] Cass., Sez. II, n. 9891/ 2011, secondo cui «Nella fattispecie in esame, l'utilizzazione della password – illecitamente ottenuta – per entrare nel sistema informatico di home banking del correntista (protetto da misure di sicurezza costituite, appunto, dai dati di accesso personali) e messo a sua disposizione dalle Poste Italiane, servì per stornare fondi dal conto corrente della C.: con il che si è verificata l'ipotesi di intervento (nella specie: ordine di bonifico dal conto corrente della C. a quello dell'imputato) senza diritto sui dati e/o informazioni (nella specie: sul saldo attivo del conto corrente) contenuti nel suddetto sistema informatico. Si può quindi concludere [...] che la fattispecie, così come contestata, rientra nell'ipotesi criminosa di cui all'art. 640 ter c.p.».

[149] FLOR, *op.cit*., p. 9.

[150] RECCIA, *op. cit*., p. 9.

alla condotta, all'art. 494 c.p.[151] piuttosto che all'art. 640 *ter* c.p. Vi sono però alcuni autori[152] che, nell'impossibilità di una riforma organica del settore, ritengono valida l'alternativa di riformulare l' art. 640 *ter* c.p. di modo che questo, oltre a rispettare i canoni di determinatezza e offensività, possa ricomprendere anche le diverse tipologie di *phishing*.

[151] SCHIPANI, *op. cit.*, p. 54 afferma che «ciò che caratterizza i *phishing attacks*, e che ci permette di ricondurre all'interno di questa unica categoria una molteplicità di attacchi informatici aventi caratteristiche diverse, è il furto d'identità digitale, ovvero l*'identity theft*».

[152] L'Autore, RECCIA, *op. cit*., p. 24, ha proposto lui stesso una possibile formulazione della norma in questo senso: «chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, anche attraverso l'induzione in errore del titolare di tali dati, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito [...]».

# CAPITOLO III

# REATI INFORMATICI CONTRO LA PERSONA: LA PORNOGRAFIA VIRTUALE E IL *REVENGE PORN*

SOMMARIO: 1. Un cenno al quadro internazionale in merito al fenomeno dello sfruttamento sessuale. – 2. La genesi dell'art 600 *ter* c.p. e il concetto di "pornografia minorile". - 2.1. La vera natura dell'art. 600 *ter*, comma 1 c.p. – 2.1.1. Le altre condotte dell'art. 600 *ter* c.p.: La divulgazione e cessione del materiale pedopornografico. – 2.2. La detenzione di materiale pedopornografico (art. 600 *quater* c.p.). - 2.3. La pornografia "virtuale". - 3. Il fenomeno del *Sexting* e la reazione della giurisprudenza. – 3.1. L'*iter* che ha portato alla criminalizzazione del *Revenge porn* (*ex* art 612 *ter* c.p.). – 3.1.1. La struttura dell'art. 612 *ter* c.p.

## 1. Un cenno al quadro internazionale in merito al fenomeno dello sfruttamento sessuale.

La lotta alla pedopornografia trova la sua origine propulsiva nelle fonti sovranazionali, quali Convenzioni internazionali e Direttive dell'Unione Europea, sul presupposto di garantire la tutela all'integrità sessuale dei minori.

L'impressione che si ricava dal comportamento adottato dal legislatore italiano è quella di un seguito con atteggiamento passivo delle direttive derivanti dagli organi sovranazionali[1], pur esistendo margini di discrezionalità a livello nazionale.

Il primo passo a livello internazionale contro ogni forma di sfruttamento sessuale dei minori è costituito dalla Convenzione ONU sui Diritti del Fanciullo (*Convention on the rights of child*) adottata a New York nel 1989 e poi ratificata in Italia nel 1991 con la Legge n. 176: essa rappresenta il primo vero documento volto a sancire espressamente l'obbligo di protezione del minore, rappresentando la prima forma di tutela concreta contro "ogni forma di sfruttamento e di abuso sessuale"[2].

Sul punto, fondamentale quanto disposto dall' art. 34: «Gli Stati parte si impegnano a proteggere il fanciullo contro ogni forma di sfruttamento sessuale e di violenza sessuale. A tal fine, gli Stati adottano in particolare ogni adeguata misura a livello nazionale, bilaterale e multilaterale per impedire: a) che dei fanciulli siano incitati o costretti a dedicarsi ad una

[1] PETRINI, *La tutela del buon costume*, in *Dir. inform*., 2011, fasc. 3, p. 4 fa espresso riferimento a un lavoro di "traduzione" in italiano delle previsioni di carattere necessariamente generale.
[2] BIANCHI, in *I confini della repressione penale della pornografia minorile. La tutela dell'immagine sessuale del minore fra esigenze di protezione e istanze di autonomia*, Torino, 2019, p. 64.

attività sessuale illegale; b) che dei fanciulli siano sfruttati a fini di prostituzione o di altre pratiche sessuali illegali; c) che dei fanciulli siano sfruttati ai fini della produzione di spettacoli o di materiale a carattere pornografico»[3]. Viene così imposto agli Stati aderenti di adottare misure volte al contrasto dello sfruttamento del minore sia nella prostituzione, che nella produzione di spettacoli e materiale pornografico.

Possono farsi due rilievi. Innanzitutto, la disposizione si riferisce a "ogni misura adeguata", lasciando quindi piena autonomia decisionale al Parlamento nazionale circa la tipologia di sanzioni da disporre[4]. In secondo luogo, l'utilizzo del termine "sfruttamento" alle lettere b) e c), non puntualmente definito, avrebbe potuto consentire all'interprete di ritenere lecite le medesime condotte nel caso non si fosse ravvisato alcuno sfruttamento e fosse coinvolto un minore considerato "maturo" per poter intrattenere rapporti sessuali ed essere rappresentato in immagini pornografiche[5].

La Convenzione ha portato all'attenzione internazionale l'importanza e la gravità del fenomeno di sfruttamento sessuale dei minori, tanto da indurre le Nazioni Unite, negli anni successivi, a istituire un apposito istituto, lo *Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography*, con il compito di analizzare e monitorare il fenomeno in questione al fine di predisporre delle misure di intervento[6].

Nel '96, a Stoccolma, i diversi Stati parteciparono a una conferenza mondiale (*First World Congress against Commercial Sexual Exploitation of Children*) volta alla predisposizione di misure concrete idonee a combattere, a livello globale, sia la prostituzione che la pornografia minorile. Dalla conclusione dei lavori di questo incontro derivarono, da una parte, la cosiddetta Dichiarazione di Stoccolma e, dall'altra, un Programma d' azione ad essa allegato.

La prima, sotto il profilo del contenuto, risulta nettamente più stringente e impegnativa rispetto alla Convenzione sopramenzionata. Infatti, l'atto impone non solo il ricorso allo strumento penale, che nel caso della Convenzione aveva rappresentato uno spazio di autonomia nazionale, ma anche la punibilità del cliente che usufruisce della prostituzione minorile e di colui che detiene materiale pedopornografico[7]. In aggiunta, oltre a definire

[3] Traduzione non ufficiale sul sito *https://www.savethechildren.it/.*
[4] PETRINI, *La tutela del buon costume*, cit., p. 5.
[5] BIANCHI, in *I confini della repressione penale della pornografia minorile, op. cit.,* p. 65.
[6] BIANCHI, *Ivi*., p. 66.
[7] SCARCELLA, *Tassatività e determinatezza della nozione di «pornografia»: la Cassazione apre al diritto comunitario*, in *Dir. pen. proc*, 2010, fasc. 8, p. 974, si afferma che il Programma d'azione contro lo sfruttamento sessuale dei bambini a fini commerciali al par. 4, enuncia le varie forme di tutela ed impegna gli Stati, tra l'altro, a introdurre norme che sanzionino anche il possesso di materiale pornografico infantile. Tuttavia, nel '97 con l'adozione, da parte del Consiglio dell'Unione europea, dell'Azione comune per la lotta

espressamente al punto 5 cosa si debba intendere per "sfruttamento sessuale di bambini a fini commerciali"[8], ossia l'oggettificazione del minore conseguente all'abuso sessuale compiuto da un adulto a fronte di una retribuzione di qualsivoglia natura, la Dichiarazione elenca gli effetti negativi derivanti dalle condotte[9], facendo emergere l'interesse centrale di questo elaborato: la tutela dello sviluppo, non solo fisico, ma anche morale e psicologico, del minore.

Il Programma d'azione, invece, ha la funzione di stimolare gli Stati verso una cooperazione internazionale per contrastare, adottando tutte le misure necessarie, come ad esempio la modifica del sistema normativo, lo sfruttamento sessuale a fini commerciali[10].

Un altro passo avanti nella lotta contro lo sfruttamento sessuale dei minori è stato compiuto con l'adozione, sulle orme della Raccomandazione del Consiglio d'Europa del 1989, della Convenzione di Budapest nel 2001, ratificata in Italia nel 2008. Centrale in questo senso è stato l'art. 9[11] in tema di pedopornografia informatica. In particolare, la disposizione non si limita a stabilire un mero obbligo in capo agli Stati di adozione di misure, aventi non solo natura legislativa, contro il fenomeno della pedopornografia, ma, al par. 2, si cura altresì di fornire, per la prima volta dopo i Protocolli alla Convenzione di New York del 2000[12], una definizione oggettiva del concetto di "pornografia infantile". L'espressione parrebbe includere «il materiale pornografico che raffigura: a. un minore coinvolto in un comportamento sessuale esplicito; b. un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito; c. immagini realistiche raffiguranti un minore

contro la tratta degli esseri umani e lo sfruttamento sessuale dei bambini, nel prescrivere l'obbligo di sanzioni «effettive, proporzionate e dissuasive» per le varie ipotesi criminose, viene fatta eccezione per le condotte di mera detenzione di materiale pornografico.

[8] Dichiarazione di Stoccolma del 1996, punto 5: «(…) Esso comprende l'abuso sessuale da parte dell'adulto e una retribuzione in natura o sotto forma di spese corrisposta al bambino o a terze persone. Il bambino viene trattato sia come oggetto sessuale che come oggetto commerciale. Lo sfruttamento sessuale dei bambini a fini commerciali rappresenta una forma di coercizione e di violenza esercitata nei confronti dei bambini ed equivale ai lavori forzati ed a una forma di schiavitù contemporanea».

[9] In questo senso si veda la Dichiarazione di Stoccolma del 1996 al punto 9.

[10] BIANCHI, in *I confini della repressione penale della pornografia minorile, op. cit.,* p. 68.

[11] Articolo 9- Reati relativi alla pornografia infantile: «1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto: a. la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico; b. l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico; c. la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico; d. il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri; e. il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici».

[12] PETRINI, *La tutela del buon costume*, cit., p. 5, il quale afferma che in base all'art. 2 dei Protocolli, il concetto di "pornografia minorile" viene definito, soggettivamente, come ipotesi in cui venga rappresentato un «bambino dedito ad attività sessuali esplicite, concrete o simulate o qualsiasi rappresentazione degli organi sessuali di un bambino soprattutto a fini sessuali».

coinvolto in un comportamento sessuale esplicito». Viene quindi equiparata per la prima volta la pedopornografia virtuale a quella reale. Tuttavia, al quarto paragrafo viene inserita una riserva[13] in favore degli Stati, i quali potranno decidere sia di non applicare le due categorie di pedopornografia "virtuale" ed "intima" citate al par. 2, lett. b) e c), ma non anche la pedopornografia "reale" di cui alla lett. a), e le due condotte previste al par. 1, lett. d) e e).

Per completezza pare corretto evidenziare che al par. 3 dello stesso art. 9, la Convenzione prosegue fornendo anche una definizione del termine "minore", in base alla quale questo «include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un'età minore, che non potrà essere inferiore ai 16 anni». Emerge nuovamente il margine di discrezionalità lasciato ai Parlamenti nazionali e l'approccio passivo frequentemente adottato dal legislatore di seguire pedissequamente le indicazioni degli atti sovranazionali, nella convinzione di dover semplicemente "tradurre" le direttive, non può giustificare la legittimità di una nuova fattispecie incriminatrice[14]. È necessario assicurare centralità all'intervento parlamentare e a tal fine provvedono le stesse Convenzioni o Direttive mediante clausole finali o di riserva che meritano di essere eseguite dal legislatore esprimendo e condividendo scelte di politica criminale[15].

Accanto alla Convenzione di Budapest, si pone poi la Convenzione di Lanzarote (*Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*) del 2007, ratificata in Italia nel 2012. Quest'ultima, a differenza della prima, ha lo scopo di far sì che le legislazioni degli Stati contemplino i delitti contro la pedopornografia senza però circoscriverli all'utilizzo di strumenti telematici e informatici. Dal preambolo della Convenzione emerge come il fine ultimo non siano solo la protezione del minore e la repressione dei fenomeni di prostituzione e pornografia minorile, ma anche la prevenzione incentrata sull'informazione della società e del minore riguardo al fenomeno e la formazione degli operatori chiamati ad interfacciarsi con le vittime[16].

---

[13] Articolo 9, par. 4 «Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1., sottoparagrafi d. ed e., e 2, sottoparagrafi b. e c.».

[14] Atteggiamento che si è verificato anche in sede di ratifica della Convenzione di Budapest, infatti, in PICOTTI, *I primi vent'anni della Convenzione di Budapest nell'ottica sostanzialista e la mancata ratifica ed esecuzione del Primo Protocollo addizionale contro il razzismo e la xenofobia*, in *Dir. pen. proc*, 2022, fasc. 8, p. 1030, si legge che il legislatore italiano, nella convinzione che obblighi di incriminazione fossero già sostanzialmente adempiuti grazie alle disposizioni già vigenti, si è limitato a rivedere le norme in materia di danneggia- menti informatici e di falsità informatiche.

[15] PETRINI, *La tutela del buon costume*, cit., p. 5.

[16] Vedi Preambolo della Convenzione di Lanzarote del 2007, in cui si legge a p. 3 «Risoluti a contribuire efficacemente alla realizzazione dell'obiettivo comune di proteggere i bambini contro lo sfruttamento e l'abuso sessuale, chiunque ne sia l'autore, e di fornire assistenza alle vittime; Tenendo conto dell'esigenza di elaborare uno strumento internazionale completo che sia incentrato sugli aspetti della prevenzione, della protezione e del

Una delle peculiarità della Convenzione è quella di aver anticipato la soglia di punibilità all'"accesso consapevole, mediante l'utilizzo delle tecnologie dell'informazione e della comunicazione, a materiale pedopornografico" (ex art. 20, par. 1, lett. f), a cui però segue al par. 4 una riserva[17].

Inoltre, se la Convenzione di Budapest prevede la possibilità per Stati di non punire le condotte previste alle lett. d) ed e) dell'art. 9, par. 1[18], e di non applicare il par. 2 quando il materiale oggetto della condotta si sostanzia in materiale pedopornografico "virtuale" o "intimo", la Convenzione di Lanzarote, invece, all'art. 20, par. 3[19], contempla un'unica causa di non punibilità riguardante la condotta di possesso e produzione aventi ad oggetto la pedopornografia virtuale e il minore che abbia raggiunto l'età del consenso.

Un'ulteriore novità rispetto agli altri strumenti sovranazionali è l'introduzione della fattispecie di adescamento di minori all'art. 23[20], indirizzata a sanzionare la condotta dell'adulto che entra in contatto con il minore con l'intenzione di realizzare uno dei reati di sfruttamento o abuso sessuale, anticipando così la soglia di punibilità ancor prima che si possa parlare di tentativo di questi stessi ultimi delitti[21].

In questa breve analisi meritano menzione, infine, la Decisione quadro 2004/68/GAI e la sostituta Direttiva 2011/93/UE. Le suddette fonti rappresentano uno strumento legislativo con un diverso *enforcement* rispetto agli altri atti sovranazionali sopramenzionati: è proprio in virtù della loro diversa forza vincolante, da cui discende anche la possibilità di azionare una procedura di infrazione in caso di inadempimento di uno Stato, che il legislatore europeo è intervenuto in materia, nonostante la preesistenza delle Convenzioni[22].

La Decisione quadro ha rappresentato un primo passo da parte dell'Unione Europea nella lotta contro lo sfruttamento sessuale dei minori con l'intento di stabilire un livello

---

diritto penale in materia di lotta contro ogni forma di sfruttamento e di abuso sessuale nei confronti dei minori e che istituisca uno specifico meccanismo di controllo (..)».

[17] Convenzione di Lanzarote del 2007, Articolo 20, par. 4: «Ogni Parte potrà riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 1.f».

[18] Convenzione di Budapest, Articolo 9, par. 1: «(…) d. il procurare pornografia infantile attraverso un sistema informatico per sé stessi o altri; e. il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici».

[19] Convenzione di Lanzarote del 2007, Articolo, 20, par. 3: «Ogni Parte potrà riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 1.a), e 1.e) alla produzione e al possesso di materiale pornografico:– consistente esclusivamente in rappresentazioni simulate o in immagini realistiche di un minore inesistente;– in cui siano rappresentati minori che hanno raggiunto l'età fissata conformemente all'Articolo 18, paragrafo 2, quando tali immagini sono prodotte e possedute da questi ultimi con il loro consenso e unicamente per loro uso privato».

[20] Recepita poi dal legislatore italiano con la Legge n. 172/2012 nel nuovo art. 609 *undecies* c.p.

[21] BIANCHI, in *I confini della repressione penale della pornografia minorile, op. cit.,* p. 76.

[22] VERRI, *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE. Approvate dal legislatore europeo nuove norme contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile*, in *Dir. pen. cont*., 2010, p. 2.

minimo di armonizzazione[23] tra le legislazioni nazionali. L'obbiettivo ultimo, come emerge dal *Considerando* 4, era quello di tutelare «il diritto fondamentale di tutti i bambini ad una crescita, un'educazione ed uno sviluppo armoniosi»[24]. La Decisione, dalla quale è poi derivata la Legge n. 38/2006 adottata in Italia, si era prefissata lo scopo di integrare le già presenti iniziative sovranazionali e incentivare la cooperazione tra gli Stati, consentendogli di adottare un approccio comune e uniforme e di prevedere «sanzioni effettive, proporzionate e dissuasive, e una cooperazione giudiziaria più ampia possibile»[25]. In tal senso, all'art. 1, lett. b), era stata prevista una definizione di "pornografia minorile", inteso come «materiale pornografico che ritrae o rappresenta visivamente: i) un bambino reale implicato o coinvolto in una condotta sessualmente esplicita, fra cui l'esibizione lasciva dei genitali o dell'area pubica; o ii) una persona reale che sembra essere un bambino implicata o coinvolta nella suddetta condotta di cui al punto i); o iii) immagini realistiche di un bambino inesistente implicato o coinvolto nella suddetta condotta»[26].

Tuttavia, con l'entrata in vigore del Trattato di Lisbona e l'evoluzione continua del fenomeno, è presto emersa l'inadeguatezza degli obbiettivi che la Decisione quadro si era posta inizialmente, non più opportuni e proporzionati all'esigenza di adottare un approccio di tipo globale[27], richiesto dai più gravi reati di sfruttamento sessuale e pedopornografia. In particolare, la Decisione non faceva riferimento alle nuove forme di aggressione attuate mediante l'informatica, e, anzi, limitava il suo campo applicativo solo a determinate fattispecie. In aggiunta, non si prendeva in considerazione la necessità di adottare misure adeguate a una giusta prevenzione e di protezione per le vittime[28].

Conseguentemente, le istituzioni ritennero opportuno procedere a una sostituzione completa della Decisione quadro con la già menzionata Direttiva 2011/93/UE, confezionata per perseguire i medesimi obbiettivi che erano stati inseriti nella Proposta di Direttiva: oltre a contrastare l'abuso e lo sfruttamento, tutelare le vittime e farsi che i reati vengano perseguiti in modo efficace.

---

[23] VERRI, *Ivi.,* p. 3.
[24] *Considerando* n. 4.
[25] *Considerando* n. 7.
[26] BIANCHI, in *I confini della repressione penale della pornografia minorile, op. cit.,* p. 77.
[27] VERRI, *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE, cit.,* p. 3.
[28] Proposta di Direttiva del Parlamento Europeo e del Consiglio relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pedopornografia, che abroga la Decisione quadro 2004/68/GAI, Relazione, punto 1 (voce "Disposizioni vigenti nel settore della proposta"), p. 3; Per un approfondimento si veda BIANCHI, in *I confini della repressione penale della pornografia minorile, op. cit.,* p. 79.

Per la prima volta è stata data dal legislatore europeo una definizione puntuale di "pornografia minorile"[29] e "spettacolo pornografico"[30], assenti nell'ordinamento italiano, e viene imposta la criminalizzazione di tre categorie di reati: i reati di abuso sessuale (art. 3); i reati di sfrutta- mento sessuale (art. 4); i reati di pornografia minorile (art. 5); il delitto di adescamento di minori per scopi sessuali[31]. Questo viene disciplinato sia dall'art. 6, che dall'art. 7, il quale sanziona l'istigazione, il favoreggiamento, il concorso e il tentativo. Questi ultimi due articoli rappresentano una novità rispetto alla Decisione quadro, in cui, appunto, non si prevedeva la penalizzazione dell'adescamento con l'ausilio delle nuove tecnologie ai fini di abuso e la visualizzazione di materiale pedopornografico via *internet* o tramite *webcam*[32].

Ulteriore elemento che merita un accenno in questa sede è l'art. 25 della Direttiva, rubricato "Misure contro i siti web che contengono o diffondono materiale pedopornografico"[33]. In sostanza, con questa disposizione si impone agli Stati di adoperarsi per chiudere tutte le pagine *web* presenti sul territorio che si occupano di distribuzione in rete di materiale pedopornografico, o quanto meno di impedirvi l'accesso. Anche in questo caso, come emerge chiaramente dal *Considerando* 47[34], la Direttiva caldeggia fortemente

[29] Art. 2, lett. d): «utilizzo di un minore per atti sessuali, dietro promessa o dazione di somme di denaro o altri vantaggi o utilità in cambio della partecipazione a tali atti, a prescindere che il pagamento, la promessa o i vantaggi siano rivolti al minore o a terzi».

[30] Art. 2, lett. e): «l'esibizione dal vivo, diretta a un pubblico, anche a mezzo di tecnologie dell'informazione e della comunicazione di: i) un minore in atteggiamenti sessuali espliciti, reali o simulati, oppure di ii) organi sessuali di un minore, per scopi prevalentemente sessuali».

[31] Chiamato anche "*grooming*", a riguardo si veda VIZZARDI, *Sull'"adescamento" di minore tramite social network e il tentativo di atti sessuali con minorenne,* in *Dir. pen. cont*, 2012, fasc. 1., p. 196 ss.

[32] VERRI, *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE, cit.,* p. 4.

[33] Art. 25: «1. Gli Stati membri adottano le misure necessarie per assicurare la tempestiva rimozione delle pagine web che contengono o diffondono materiale pedopornografico ospitate nel loro territorio e si adoperano per ottenere la rimozione di tali pagine ospitate al di fuori del loro territorio; 2. Gli stati possono adottare misure per bloccare l'accesso alle pagine web che contengono o diffondono materiale pedopornografico agli utenti internet sul loro territorio. Tali misure devono essere stabilite con procedure trasparenti e devono fornire idonee garanzie, in particolare al fine di assicurare che la restrizione dia limitata allo stretto necessario e proporzionata e che gli utenti siano informati del motivo della restrizione. Tali garanzie includono la possibilità di ricorrere per via giudiziaria».

[34] Secondo il quale, «Tuttavia, malgrado questi sforzi, spesso non è possibile eliminare alla fonte il contenuto pedopornografico quando il materiale originale non è situato nell'Unione, perché lo Stato che ospita i server non è disposto a cooperare, ovvero perché il processo per ottenere l'eliminazione del materiale dallo Stato interessato si rivela particolarmente lungo. È anche possibile istituire meccanismi che impediscano l'accesso, dal territorio dell'Unione, alle pagine internet che contengono o diffondono materiale pedopornografico. Le misure adottate dagli Stati membri in conformità della presente direttiva al fine di eliminare o, se del caso, bloccare i siti web contenenti pornografia minorile potrebbero essere basate su vari tipi di azione pubblica, comprese azioni legislative, non legislative, giudiziarie o di altra natura. In tale contesto, la presente direttiva non pregiudica l'azione volontaria avviata dal settore internet per evitare abusi dei suoi servizi, o qualsiasi sostegno da parte degli Stati membri nei confronti di tale azione. Qualunque sia la modalità di azione o il metodo scelto, gli Stati membri dovrebbero accertarsi che sia garantito un adeguato livello di certezza del diritto e di prevedibilità giuridica per gli utenti e i fornitori di servizi. Sia per eliminare che per bloccare i materiali pedopornografici, è opportuno stabilire e rafforzare la cooperazione tra autorità pubbliche, soprattutto

la collaborazione tra i diversi Paesi, soprattutto con i Paesi terzi qualora vi sia la necessità di eliminare siti che trovano la loro collocazione in un *server* fuori dall'Unione.

## 2. La genesi dell'Art 600 *ter* c.p. e il concetto di "pornografia minorile".

Il fenomeno dell'abuso sessuale *online* si compone di tutte quelle fattispecie che riguardano la cosiddetta "pedopornografia *online*" facendo riferimento a situazioni caratterizzate dal "coinvolgimento di un minore in attività sessuali, virtuali o reali, attraverso gli strumenti offerti dalle nuove tecnologie"[35]. Sostanzialmente, il luogo del reato e lo strumento utilizzato per la diffusione delle immagini vengono rappresentati entrambi dallo strumento telematico o informatico.

La commissione di questa tipologia di reati deriva da quella forma di devianza o perversione sessuale che si concretizza nell'attrazione provata da un adulto nei confronti di un fanciullo, cosiddetta pedofilia. Già con il Codice Rocco era stato incriminato il rapporto sessuale con minori, ma con il tempo e, soprattutto, con l'avanzamento di *internet* e lo sviluppo costante delle tecnologie offerte alla società, il legislatore ha dovuto prendere coscienza delle insidiosità e capacità diffusive di questo fenomeno. Infatti, il forte utilizzo dei *personal computer* e la facilità con cui le persone possono oggi dar vita a nuove relazioni sulla rete, hanno fatto sì che le pratiche di distribuzione e di divulgazione e la possibilità di procurarsi materiale pedopornografico risultassero semplificate, consentendo anche una tutela maggiore dell'anonimato[36].

Le fattispecie criminose oggetto di analisi hanno subito una forte evoluzione nel corso del tempo, proprio in virtù dei cambiamenti che hanno riguardato le condotte materiali realizzate in rete. Se prima si puniva la condotta attiva dell'autore nei confronti del minore

affinché sia assicurata l'esaustività degli elenchi nazionali dei siti web a contenuto pedopornografico e siano evitate duplicazioni. Tutti questi sviluppi devono tenere conto dei diritti dell'utente finale e rispettare le procedure giuridiche e giudiziarie vigenti, e la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e la Carta dei diritti fondamentali dell'Unione europea. Il programma «Internet più sicuro» ha istituito una rete di linee telefoniche dirette, allo scopo di raccogliere informazioni e garantire la copertura e lo scambio di segnalazioni dei contenuti illeciti on line».

[35] Definizione utilizzata da SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale*, in *Diritto penale dell'informatica: reati della rete e sulla rete*, a cura di PARODI – SELLAROLI, Milano, 2020, p. 279.

[36] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica*, in *Il diritto penale delle nuove tecnologie*, Milano, 2007, p. 141.

passivo, oggi, la rilevanza penale è stata estesa a ipotesi in cui è lo stesso minore a prendere attivamente parte nel reato[37].

Gli artt. 600 *bis* c.p. e seguenti sono stati originariamente inseriti nel codice, in adesione alle iniziative internazionali, con la Legge n. 269 del 1998[38] nella sezione I del capo III del titolo XII del libro II del Codice penale. In particolare, agli obblighi internazionali derivanti dalla Convenzione dell'89, era stata fornita risposta con l'introduzione nel codice degli artt. 600 *bis*, comma 1 c.p., 600 *ter* c.p., 600 *quinques*, mentre l'aggiunta ulteriore degli artt. 600 *bis*, comma 2 c.p. e 600 *quater* c.p., ha rappresentato il frutto di una scelta di politica criminale volta a contrastare primariamente le condotte di "produzione" del materiale pedopornografico e così anche lo sfruttamento sessuale[39]. Deve sottolinearsi come l'impatto più significativo della legge abbia riguardato proprio la diffusione e detenzione di questa tipologia di immagini mediante strumenti informatici e telematici[40].

Con la già menzionata legge si è cercato, da un lato, di raffinare gli strumenti messi a disposizione per la ricerca della prova[41], istituendo anche il nuovo Servizio di Polizia postale e delle Telecomunicazioni[42], e, dall'altro, di implementare l'impianto normativo con nuove fattispecie penali capaci di punire i comportamenti "tipici" dei pedofili prendendo in considerazione e analizzando dati reali[43].

La norma centrale con cui è stata introdotta nel '98 la nozione di "pornografia minorile" è l'art. 600 *ter* c.p. Si tratta di una disposizione decisamente complessa, che enuclea diverse

---

[37] In questo senso SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale, op. cit.,* p. 279. Ci sono dei casi, come il *sexting,* in cui il reo adesca il fanciullo online, cercando di carpirne la fiducia, così che quest'ultimo sia portato a riprendere ed inviare immagini di comportamenti sessualmente espliciti.

[38] "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori", detta anche Legge antipedofilia.

[39] DE NATALE, *Pornografia minorile e internet. Brevi note sui primi orientamenti dottrinali e giurisprudenziali*, in *Riv. pen*., 2004, fasc. 3, p. 1.

[40] SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale, op. cit.,* p. 280. Nello stesso senso DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op. cit.,* p. 142 e GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale*, in *I reati informatici in ambito relazionale e a sfondo sessuale. Cyberstalking, cyberbullismo e pedopornografia online*, Torino, 2021, p. 148.

[41] DE NATALE, *Pornografia minorile e internet, cit.,* p. 1, parla della facoltà assicurata agli organi inquirenti di avvalersi degli stessi strumenti utilizzati per la mafia e il traffico internazionale di stupefacenti come, ad esempio, le intercettazioni telefoniche, l'acquisto simulato, siti trappola o ancora l'utilizzo di infiltrati.

[42] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op. cit.,* p. 142, è un organo istituito ad opera del ministro dell'Interno, presso le sedi delle Questure italiane, consistente in un nucleo di polizia specializzato a cui è stata affidata, in certi casi anche in via esclusiva, la facoltà di compiere indagini per questa tipologia di reati.

[43] SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale, op. cit.,* p. 280. Per un approfondimento sul Cyberpedofilo si veda GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 152.

condotte autonome, punite con sanzioni variabili, la cui finalità è quella di tutelare il libero sviluppo psico- fisico del minore[44].

Nonostante il già menzionato articolo abbia subito diverse modifiche nel corso degli anni, la sua struttura è rimasta sostanzialmente immutata. Infatti, in tutte le sue versioni, la disposizione prima punisce la condotta più grave di produzione di materiale pornografico e poi, ai commi 3 e 4, punisce le condotte sussidiarie[45], nonché meno gravi, di divulgazione, distribuzione e cessione.

Oggi, l'art. 600 *ter* c.p. punisce tre distinte ipotesi delittuose. Con la prima, al comma 1, viene sanzionato «Chiunque, utilizzando[46] minori degli anni diciotto, realizza esibizioni pornografiche o produce materiale pornografico ovvero induce minori di anni diciotto a partecipare ad esibizioni pornografiche» e alla stessa pena soggiace «chi fa commercio del materiale pornografico». In seconda istanza, il comma 3 punisce: «Chiunque..., con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde[47] o pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga, diffonde notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto». Da ultimo, il comma 4[48], sanziona, invece, la condotta di colui che cede, anche a titolo gratuito, detto materiale. Nel 2006 il legislatore ha aggiunto un'aggravante ad effetto speciale[49] in caso di "ingente quantità", escludendone però l'applicazione nei casi di cui al primo comma[50]. Nel 2012, infine, è stato introdotto l'ultimo comma[51] fornendo così una definizione di "materiale pornografico".

Per quanto concerne la definizione di materiale pedopornografico, non era contenuta né nella legge del '98[52], né in quella del 2006. Tuttavia, la giurisprudenza[53] aveva affermato

---

[44] Vedi Preambolo della Legge n. 269/1998.
[45] Sussidiarietà che emerge dall'utilizzo della clausola «al di fuori delle ipotesi di cui al primo e al secondo Comma».
[46] Termine che ha sostituito il precedente verbo "sfruttare" con la novella del 2006.
[47] La condotta di diffusione è stata introdotta con la novella del 2006.
[48] Art. 600 *ter*, comma 4 (sostituito nel 2006): «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».
[49] SCARCELLA, *Tassatività e determinatezza della nozione di «pornografia, cit.,* p. 975.
[50] Art. 600 *ter*, comma 5: «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».
[51] Art. 600 *ter*, comma 8: «Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, 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».
[52] SCARCELLA, *Tassatività e determinatezza della nozione di «pornografia», cit.,* p. 975. Dal disegno di legge e dai lavori preparatori emerge che, in realtà, l'assenza di una definizione sarebbe più una scelta consapevole, che una dimenticanza. Infatti, si era evidenziato come questa scelta fosse dipesa dalla difficoltà di elaborare una nozione astratta a prescindere dal contesto e dai comportamenti posti in essere in concreto.
[53] Trib. Perugia nel 8 luglio 2003.

che «la natura pornografica della rappresentazione di minori, in pose che ne lascino scoperti integralmente o parzialmente gli organi sessuali, al fine di distinguerla dal materiale di natura diversa, deve essere individuata in base all'accertamento della destinazione della rappresentazione ad eccitare la sessualità altrui e della sua idoneità ha detto scopo». In accordo a questa affermazione, si deve precisare che ci sono casi in cui immagini ritraenti parti del corpo di per sé non erogene assumono carattere pornografico qualora idonee a stimolare l'eccitazione altrui. Infatti, anche in queste ipotesi si realizzano la lesione e lo sfruttamento dell'infanzia, quale bene giuridico tutelato dalla norma[54]. La stessa pronuncia afferma poi che «non sarebbe pornografica solo un'immagine ricavata da un contesto lucido ed accessibile ad una cerchia determinata di persone, come quella di chi scatti una foto ad un figlio o ad un nipote che fa il bagno[55]».

La svolta a riguardo è avvenuta con la Legge n. 172/ 2012 (Ratifica della convenzione di Lanzarote per la protezione dei minori contro lo sfruttamento e l'abuso sessuale), che ha apportato diverse modifiche[56] e integrazioni all'art. 600 *ter* c.p. In particolare, è stato aggiunto il concetto di "pornografia minorile" nel nuovo comma 7[57], riprendendo la definizione che era stata fornita all'art. 20, par. 2[58] della Convenzione di Lanzarote. Ad oggi, quindi, come affermato anche dalla Corte di Cassazione[59], costituisce materiale pedopornografico «la rappresentazione, con qualsiasi mezzo atto alla conservazione virgola di atti sessuali espliciti coinvolgenti soggetti minori di età, oppure degli organi sessuali di minori con modalità tali da rendere manifesto il fine di causare concupiscenza od ogni altra pulsione di natura sessuale nonché una qualunque rappresentazione degli stessi organi per scopi sessuali»[60].

---

[54] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 143.
[55] DESISTO – DEZZANI – SANTORIELLO, *Ibidem.*
[56] Con la sostituzione del primo comma la legge, oltre a ridurre leggermente l'entità della pena pecuniaria, integra la condotta che costituisce reato. In particolare: aggiunge alle esibizioni pornografiche il concetto di spettacoli pornografici; aggiunge al concetto di induzione alla pornografia minorile quello di reclutamento; prevede la sanzionabilità anche di colui che, a prescindere da tali condotte attive, tragga comunque profitto da tali esibizioni e spettacoli.
[57] Il comma 7 recita: «Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, 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».
[58] Convenzione di Lanzarote del 2007, art. 20, par. 2: «Ai fini del presente articolo, il termine "pornografia minorile" indica qualsiasi materiale che ritrae o rappresenta visivamente un bambino impegnato in atti sessuali espliciti, reali o simulati, o qualsiasi rappresentazione di organi sessuali di bambini a fini essenzialmente sessuali».
[59] Cass., Sez. V., n. 33862/2018 e Cass., Sez. III., n. 5874/2013.
[60] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 163.

Rispetto alla definizione che era stata fornita all'art. 2 dei Protocolli opzionali alla Convenzione di New York del 2000[61], quella introdotta dall'art. 4, comma 1, lett. h) della legge del 2012 risulta più rigorosa. Infatti, anche la Corte nel 2013[62] ha affermato come in base a questa basti la rappresentazione "per scopi sessuali" degli organi genitali del minore e non si esiga più l'esibizione lasciva degli stessi[63].

Inoltre, il carattere pedopornografico, non solo non presuppone una partecipazione consapevole del minore[64], ma la sua valutazione è competenza del giudice, il quale potrà avvalersi degli ordinari mezzi di prova senza dover necessariamente prendere in esame il materiale[65].

### 2.1. La vera natura dell'art. 600 *ter,* comma 1 c.p.

Nella sua versione originale, il comma 1 conteneva la locuzione "sfrutta", che secondo la linea di pensiero prevalente si doveva intendere quale "sfruttamento sessuale ai fini commerciali", implicando la necessità di un ritorno economico per l'integrazione del delitto. Tuttavia, questa ricostruzione letterale[66] non è parsa condivisibile.

Partendo dal presupposto che una retribuzione non varrebbe ad eliminare il pregiudizio causato al minore a seguito di queste condotte, è logico ritenere configurato il reato a prescindere dal fatto che l'autore abbia conseguito un vantaggio economico quantificabile. In questi casi, infatti, si è sempre in presenza di una "mercificazione del minore" idonea a impattare negativamente sullo sviluppo psico- fisico del fanciullo[67].

Secondo un'altra ricostruzione, il termine "sfruttamento" dovrebbe essere interpretato in senso più ampio, così da ricomprendere non solo una finalità prettamente economica, ma anche egoistica e libidinosa per la quale il minore viene strumentalizzato[68].

---

[61] La definizione recitava «bambino dedito ad a attività sessuali esplicite, concrete o simulate o qualsiasi rappresentazione degli organi sessuali di un bambino soprattutto a fini sessuali».
[62] Cass., Sez. III, n. 3110/2013.
[63] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile*, in *Dir. pen. proc*, 2019, fasc. 12, p. 1723.
[64] Cass., Sez. III., n. 42964/2015: secondo la Corte il carattere pedopornografico può essere individuato anche nella rappresentazione di movimenti, inconsapevoli e involontari, in cui i minori assumono posizioni che si concretizzano in atteggiamenti lascivi ed eroticamente eccitanti.
[65] Cass., Sez. III., n. 3110/2013.
[66] PITTARO, *Le norme di diritto penale sostanziale*, in *Dir. pen. proc*, 1998, fasc. 10, p. 1226.
[67] DE NATALE, *Pornografia minorile e internet, cit.,* p. 3.
[68] PECCIOLI, *Un ulteriore intervento a tutela dei minori (I parte*), in *Dir. pen. proc*, 2013, fasc. 3, p. 143.

Sul punto si sono pronunciate le Sezioni Unite nel 2000[69] sottolineando come il termine debba essere inteso come «strumentalizzazione dei minori a fini egoistici in modo tale da mettere in pericolo il loro libero sviluppo personale». La Suprema Corte nel pronunciarsi ha fornito anche delle indicazioni con riguardo alla natura del reato *de quo*. Infatti, con l'affermazione in base alla quale con il comma 1 dell'art. 600 *ter* l'ordinamento appresta un'anticipazione della tutela della libertà sessuale, punendo quei comportamenti prodromici che mettono a repentaglio lo sviluppo personale del minore con la sua mercificazione e immissione nel circuito perverso della pedofilia, ha statuito la natura di reato di pericolo concreto della norma. Detto in altri termini, la condotta di colui che utilizzi il minore per spettacoli o per produrre materiale pornografico sarà punibile solo qualora abbia una "consistenza tale da implicare concreto pericolo di diffusione del materiale prodotto". Nella stessa pronuncia le SS.UU avevano anche precisato che sarebbe stato compito del giudice, mediante l'ausilio di elementi sintomatici della condotta[70], accertare caso per caso la configurabilità del pericolo. Qualora, invece, le immagini fossero state destinate a rimanere nella sfera privata dell'autore, allora avrebbe potuto trovare applicazione l'art. 600 *quater* c.p.

Sulla base di questo *dictum,* era diventata molto frequente la richiesta delle difese di riqualificare il delitto in quello meno grave di detenzione di materiale pedopornografico, proprio facendo leva sull'assenza del concreto pericolo di diffusione. Una simile prospettazione è diventata non più praticabile a seguito della modifica intervenuta con la Legge n. 38/2006[71].

Punto cruciale di quest'ultima novella è stato l'aver sostituito il termine "sfruttamento" con quello di "utilizzazione". Questa modifica, infatti, ha evidenziato come sia sufficiente ai fini della configurazione del reato il semplice coinvolgimento del minore, aprendo così la

[69] Cass., SS.UU., n. 13/2000 (Sentenza Bove): nel caso di specie, ossia di un soggetto il quale aveva realizzato e detenuto, per uso affettivo, delle immagini pornografiche di un minore consenziente, la corte ha escluso il concreto pericolo di diffusione del materiale.

[70] SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale, op. cit.,* p. 286, fa un'elencazione di questi elementi sintomatici: «esistenza di una struttura organizzativa anche rudimentale atta a corrispondere alle esigenze di mercato dei pedofili, il collegamento della gente con soggetti pedofili potenziali destinatari del materiale pornografico, la disponibilità materiale di strumenti tecnici di riproduzione e/o trasmissione, anche telematica idonea a diffondere il materiale pornografico in cerchie più o meno vaste di destinatari, l'utilizzo contemporaneo o differito nel tempo di più minori per la produzione di materiale pornografico, i procedimenti penali, la condotta antecedente e le qualità soggettive del reo, quando si hanno connotati dalla diffusione commerciale di pornografia minorile nonché gli altri indizi significativi suggeriti dall'esperienza».

[71] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 165.

via ad una giurisprudenza che gli garantisca una maggiore tutela[72]. Intendendo il già menzionato termine come "degradazione del minore"[73], il fatto che la vittima sia "avvezza" alla divulgazione di sue immagini pornografiche non costituisce un'esimente: si ritiene comunque riscontrabile il requisito dell'utilizzazione. Allo stesso modo, la mera partecipazione del minore a esibizioni pornografiche comporta la realizzazione del reato, in quanto il suo coinvolgimento comporta una degradazione della sua personalità[74]. Il fine ultimo del legislatore è stato, infatti, quello di sanzionare qualunque tipo di condotta che comportasse una mercificazione del minore, indipendentemente da una finalità di lucro o uno scopo commerciale[75]. Infine, ai fini della configurabilità del reato, le condotte di "produzione" e di "esibizione", previste al comma 1, devono essere inserite in un «contesto di organizzazione almeno embrionale e di destinazione, anche potenziale, del materiale pornografico alla successiva fruizione da parte di terzi»[76].

Dopo la sentenza del 2000, e vista l'evoluzione tecnologica, la giurisprudenza è stata portata a ravvisare sempre più frequentemente il pericolo di diffusione del materiale. A titolo di esempio, è stata riconosciuta la rilevanza penale della condotta di colui che, al fine di persuadere e corrompere, ha inviato immagini pedopornografiche su "*WhatsApp*" ai minori oggetto delle sue mire sessuali[77]. Ancora, è stato ritenuto sanzionabile l'inserimento delle immagini all'interno di una cartella elettronica accessibile anche da terzi mediante il programma "*eMule*"[78]. Queste pronunce mostrano la tendenza ad escludere dal campo applicativo della norma tutte quelle ipotesi in cui il materiale sia destinato *ab origine* ad un uso strettamente personale[79].

Nel 2018 le Sezioni Unite[80] sono intervenute per rimediare alla lettura del concetto di "produzione" inteso come realizzazione di materiale destinato alla diffusione, statuendo che «ai fini dell'integrazione del reato di cui all'articolo 600 *ter*, comma 1, n. 1 c.p., con riferimento alla condotta di produzione di materiale pedopornografico, non è più necessario, viste le nuove formulazioni della disposizione introdotte a partire dalla legge 6 Febbraio 2006, n. 38, l'accertamento del pericolo di diffusione del suddetto materiale»,

[72] MANNA - RESTA, *I delitti in tema di pedopornografia, alla luce della legge 38/2006. Una tutela virtuale?* in *Dir. Int.*, 2006, fasc. 3, p. 226.
[73] Cass., Sez. III, n. 1509/2018; Conforme a Cass., Sez. III, n. 34162/2018 e Cass., Sez. III, n. 1783/2016.
[74] Cass., Sez. III, n. 10068/2008.
[75] Cass., Sez. III, n. 33862/2018 e GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile*, cit., p. 1723.
[76] Cass., Sez. III, n. 21392/2010.
[77] Cass., Sez. III., n. 37835/2017.
[78] Cass., Sez. III., n. 33298/2016.
[79] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile, cit.,* p. 1725.
[80] Cass., SS.UU., n. 51815/2018.

riqualificandolo come reato di danno. In sostanza, la Corte, vista la diffusione di nuovi strumenti tecnologici e il forte utilizzo degli *smartphones* o *tablet*, capaci di collegare in modo istantaneo l'utente alla rete *internet* e ai vari programmi di condivisione, hanno ritenuto che il requisito del pericolo di diffusione fosse privo di significato, essendo ormai «potenzialmente diffusiva qualsiasi produzione di immagini e video».

Questa pronuncia ha il merito di aver reso palese ciò che già era l'intenzione del nostro legislatore nel 2006. L'aver inserito il termine "utilizzazione" trovava la sua *ratio* nell'eliminazione del presupposto del pericolo di diffusione, intento che era passato in sordina sino al 2012, momento in cui si è inserita la definizione di "materiale pedopornografico". Quest'ultimo intervento, infatti, ha portato alla luce la concreta finalità dell'art. 600 *ter* c.p., ossia tutelare lo sviluppo della sessualità, la dignità e personalità del minore, tutti beni che verrebbero colpiti già all'atto di realizzazione del materiale pedopornografico[81].

È inoltre opportuno precisare che, secondo la giurisprudenza recente, l'utilizzazione del minore può anche assumere le forme dell'istigazione o induzione. Questi sono i casi in cui il minore, diventato "autore mediato", realizza una condotta attiva di produzione non per sua volontà, ma perché abbindolato dall'agente[82].

Per quanto riguarda il tema della "pornografia domestica", ossia i casi in cui viene prodotto del materiale pornografico, coinvolgente minori che abbiano raggiunto l'età del consenso sessuale, a uso strettamente personale, la giurisprudenza ha per tanto tempo escluso l'applicabilità dell'art. 600 *ter* c.p. per insussistenza del pericolo di diffusione. A seguito della riforma del 2012, stabilire la punibilità di questa fattispecie sarebbe in linea con la *ratio* della legge: infatti, si anticiperebbe la soglia della rilevanza penale a condotte che potrebbero costituire presupposto di quelle successive di diffusione verso terzi del materiale. Alla stessa conclusione si arriverebbe guardando alla definizione introdotta al comma 8 dell'art. 600 *ter* c.p., la quale incentra il pregiudizio allo sviluppo psico- fisico del minore sul fatto che questi venga utilizzato per compiere o subire abusi sessuali, al fine di appagare l'eccitazione altrui, anche senza un tornaconto economico. Infine, il fatto che il legislatore italiano non abbia

[81] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile, cit.,* p. 1726.
[82] Cass., Sez. III, n. 26862/2019.

esercitato la riserva riconosciutagli dall'art. 20 della Convenzione di Lanzarote[83], porta a ritenere plausibile la rilevanza penale della pornografia domestica[84].

Il nuovo inquadramento sistematico e la necessità di non estendere eccessivamente la tutela penale a fatti privi di grave disvalore hanno indotto a ritenere che il *diescrimen* tra fatti penalmente rilevanti e irrilevanti si incentri sul concetto di "utilizzazione" del minore, inteso come strumentalizzazione di quest'ultimo, e sulla effettiva configurazione di questo[85].

### 2.1.1. Le altre condotte dell'art. 600 *ter* c.p.: La divulgazione e la cessione di materiale pedopornografico.

L'art. 600 *ter* c.p., al comma 3[86], si occupa espressamente di sanzionare quelle condotte volte alla diffusione del materiale pedopornografico mediante l'utilizzo di strumenti informatici. La norma, nel punire le condotte alternative di "divulgazione, distribuzione o pubblicizzazione", utilizza una pluralità di termini generici e ampi così da estendere il più possibile la propria portata applicativa[87]. Ciò che accomuna queste condotte è la volontà di far sì che il materiale arrivi a una pluralità di persone: di conseguenza l'intento del legislatore, con questo comma, è proprio quello di colpire qualsiasi tipologia di diffusione del materiale[88].

Occorre precisare che ai fini della configurabilità del reato, sono esclusi i soggetti che hanno partecipato alla realizzazione del materiale: ciò lo si evince dalla clausola iniziale «al di fuori delle ipotesi di cui al primo e al secondo comma», la quale ne definisce il carattere residuale rispetto al comma 1[89].

Volendo distinguere queste diverse modalità di azione, per "divulgazione" si intende la messa in circolazione del materiale e l'accessibilità a quest'ultimo da parte di un numero

---

[83] Art. 20, comma 3: «Ogni Parte potrà riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 1.a), e 1.e) alla produzione e al possesso di materiale pornografico: consistente esclusivamente in rappresentazioni simulate o in immagini realistiche di un minore inesistente; in cui siano rappresentati minori che hanno raggiunto l'età fissata conformemente all'Articolo 18, paragrafo 2, quando tali immagini sono prodotte e possedere da questi ultimi con il loro consenso e unicamente per loro uso privato».
[84] PECCIOLI, *Un ulteriore intervento a tutela dei minori (I parte*), *cit*., p. 144.
[85] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile, cit.,* p. 1727.
[86] Art. 600 *ter*, comma 3: «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».
[87] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 146.
[88] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile, cit.,* p. 1727.
[89] GIORDANO, *L'evoluzione giurisprudenziale del reato di pornografia minorile, cit.,* p. 1727 e Cass., Sez. III, n. 34357/2017.

indeterminato di soggetti[90]. La Corte di Cassazione, in una sentenza degli anni 2000, ha affermato che ai fini della configurabilità della condotta è richiesta "l'esistenza di un mezzo di diffusione comunque accessibile ad una indefinita pluralità di utenti, per il cui tramite il soggetto mette a disposizione degli stessi materiale vietato o informazioni"[91]. In linea con questo requisito, il comma 3 è stato ritenuto applicabile nel caso dell'utilizzo delle *chat line*[92], per le quali, però, la Cassazione ha specificato la necessità che consentano all'utente la condivisione degli archivi, dei documenti e delle cartelle contenenti il materiale illecito così da essere potenzialmente accessibile, senza particolari formalità, da chiunque[93]. Qualora, invece, le immagini risultino oggetto di uno scambio privato, sarà applicabile il comma 4.

La rilevanza penale è stata riconosciuta anche nella condotta di divulgazione mediante programmi di scaricamento automatico da *internet* (ad esempio, da *eMule*)[94], la quale però presuppone che i *files* risultino interamente visionabili e scaricati, lasciati volontariamente nella cartella per la condivisione[95]. Nel caso di utilizzo di programmi di *file sharing*, il reato è stato escluso solo quando la fattispecie difetti di elementi sintomatici della volontà del soggetto agente di divulgare il materiale[96]. Ad esempio, nel 2012 la Cassazione[97] ha ritenuto non applicabile il comma 3, ma tutt'al più l'art. 600 *quater* c.p., nel caso di perdita accidentale della "*memory card*" per telefoni, contenente le immagini illecite, ritenendo assente la volontà del reo di consentire la fruizione di terzi. In particolare, la Corte ha ritenuto che la volontà divulgativa debba essere valutata in base al comportamento concreto dell'agente, non potendo essere desunta in modo automatico dalla mera volontà di quest'ultimo di procurarsi e detenere i *files*[98].

La "distribuzione", invece, fa riferimento a una consegna fisica dei *files*, i quali possono essere contenuti, ad esempio, in *floppy disk, dvd o cd-rom*[99]. Se per la divulgazione è certo che i destinatari del materiale pedopornografico debbano essere indeterminati, per quanto

---

[90] CARINGELLA – DE PALMA – FARINI – TRINCI, *Manuale di diritto penale: parte speciale*, Roma, 2017, p. 1046.
[91] Cass., Sez. III, n. 1762/2000.
[92] Consiste in uno spazio virtuale strutturato in canali, nella quale un solo *"nickname*", necessari ad accedere alla cartella- immagini o video, venga utilizzato da più persone alle quali siano state rese note la *username* e la *password*, le quali possono in tal modo ricevere trasmettere materiale pedopornografico.
[93] Cass., Sez. III, n. 1762/2000.
[94] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 174, *eMule* è un esempio di programma di *file- sharing*.
[95] Cass., Sez. III, n. 11169/2008.
[96] Cass., Sez. III, n. 14001/2017.
[97] Cass., Sez. III, n. 40847/ 2012.
[98] Cass., Sez. III, n. 33157/2012.
[99] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 147.

riguarda la condotta di distribuzione, è ancora dubbio se questa debba essere destinata a una *élite* di pedofili[100], ad esempio, o a più persone determinate[101].

Nel 2006 è stata poi introdotta la condotta di "diffusione" al fine di «escludere qualsiasi vuoto di tutela rispetto alla repressione delle condotte diffusive del materiale pornografico»[102], anche se rimane dubbia la sua portata innovativa, dato che il comma già puniva ogni tipo di condotta diffusiva[103].

L'ultima condotta punita è quella di "pubblicizzazione", che si risolve nel «portare tale materiale a effettiva conoscenza di una pluralità più o meno ampia, determinata o indeterminata, di destinatari»[104], mirando in questo modo a limitare l'aumento della domanda del materiale pornografico e quindi anche la produzione di quest'ultimo.

In generale, il reato di cui all'art. 600 *ter*, comma 3 c.p., si consuma nel momento in cui il materiale viene immesso nella rete, essendo possibile per un numero indeterminato di soggetti accedere alle immagini[105]. Conseguentemente, sarà da considerare irrilevante la successiva cancellazione dei *files*[106].

La seconda e ultima ipotesi sanzionata al comma 3 è quella che sanziona la condotta di distribuzione o divulgazione di notizie od informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori. Si tratta di un reato di pericolo astratto che mira a punire condotte prodromiche rispetto a quelle sanzionate agli altri commi dell'art. 600 *ter c.p.*[107]. Dal dato normativo si evince come l'oggetto materiale della condotta sia costituito dalle «notizie od informazioni finalizzate all'adescamento o sfruttamento dei minori». A riguardo, la giurisprudenza non ha ritenuto necessario che queste siano caratterizzate da veridicità o novità: è sufficiente la loro idoneità a portare alla realizzazione di ipotesi di sfruttamento sessuale o adescamento[108].

---

[100] ROMANO, *Delitti contro la sfera sessuale della persona*, Padova, 2017, p. 187.
[101] PICOTTI, *Commento all'art. 600-ter, III e IV comma c.p.*, in *Commentario delle norme contro la violenza sessuale e la pedofilia*, a cura di CADOPPI, Padova, 2006, p. 191. Nello stesso senso MANNA - RESTA, *I delitti in tema di pedopornografia, cit.,* p. 228.
[102] Relazione al d.d.l. n. C-4599, presentato alla Camera dei deputati in data 13 gennaio 2004, p. 4, pubblicato sul sito ufficiale della Camera dei deputati: www.camera.it.
[103] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 148.
[104] PICOTTI, *Commento all'art. 600-ter, III e IV comma c.p.*, op. cit., p. 189.
[105] Cass., Sez. III, n. 25232/2005.
[106] Cass., sez. III, n. 41231/ 2018.
[107] MANNA - RESTA, *I delitti in tema di pedopornografia, cit.,* p. 229.
[108] Cass., Sez. III, n. 15927/ 2009.

Il comma 4[109] si apre, anch'esso, con una clausola di riserva che ne definisce il carattere sussidiario e ne esclude l'applicazione quando le condotte sono riconducibili ai commi precedenti. In questa parte di disposizione si mira a sanzionare tutti quei comportamenti volti alla cessione a terzi determinati del materiale pedopornografico. Nel 2006, in esecuzione all'obbligo di incriminazione ex art. 3, comma 1, lett. c) della Decisione quadro del 2004, è stata introdotta anche la condotta di "offerta", equiparandola a quella di cessione. Per una parte della dottrina[110], questa modifica consisterebbe in un'anticipazione della soglia di punibilità.

Come già accennato, questo comma rappresenta un'ipotesi delittuosa di minor gravità rispetto a quelle contenute nei commi precedenti: ciò discende dal fatto che in caso di cessione, il materiale viene inviato a un numero di soggetti determinati, di conseguenza colui che lo invia continua a mantenere un certo livello di controllo, mentre, nel caso del terzo comma, i destinatari sono indeterminati comportando una lesione maggiore al bene tutelato.

Il reato di cui al quarto comma si consuma nel momento in cui il materiale viene recepito o l'offerta perviene al destinatario.

Prima del 2006, con riferimento alla condotta di cessione, era inserito il termine "consapevolmente", il quale comportava l'esclusione del dolo eventuale[111]. Infatti, parte della dottrina dava all'avverbio la funzione di escludere dal campo di applicazione del comma tutte quelle condotte in cui vi fosse un dubbio sull'avvenuto sfruttamento di un minore di diciotto anni[112]. Con l'avvenuta abrogazione dell'avverbio, il reato è pacificamente configurabile a titolo di dolo eventuale: è sufficiente che l'agente si prospetti anche solo il rischio, accettandolo, che il materiale sia pedopornografico e che la sua condotta porti alla cessione di quest'ultimo[113].

La distinzione, quindi, tra il comma 3 e il comma 4, si sostanzia nel tipo di intento diffusivo. I casi che rientrano nel novero del comma 4[114] sono caratterizzati da un intento diffusivo "chiuso" e, conseguentemente, i contenuti illeciti vengono indirizzati a una cerchia di soggetti determinati. Invece, nel caso del comma 3, l'intento diffusivo è "aperto" e quindi

---

[109] Art. 600 *ter*, comma 4: «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».

[110] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 152. Secondo altri, invece, di tratterebbe di una deroga al principio dell'istigazione non accolta

[111] MANNA - RESTA, *I delitti in tema di pedopornografia, cit.,* p. 229.

[112] DESISTO – DEZZANI – SANTORIELLO, *Ivi.,* p. 153.

[113] DESISTO – DEZZANI – SANTORIELLO, *Ibidem.*

[114] A tiolo di esempio, la sussistenza del reato è stata riconosciuta nel caso di invio, tramite posta elettronica, di immagini pedopornografiche (Cass., Sez. III, n. 5397/2001).

strutturato di modo da utilizzare la naturale capacità diffusiva della rete internet a un numero indistinto di destinatari[115].

### 2.2. La detenzione di materiale pedopornografico (ex art. 600 *quater* c.p.).

L'art. 600 *quater* c.p. punisce «Chiunque, al di fuori delle ipotesi previste nell'articolo 600ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a tre anni o 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. Fuori dei casi di cui al primo comma, chiunque, mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione, accede intenzionalmente e senza giustificato motivo a materiale pornografico realizzato utilizzando minori degli anni diciotto è punito con la reclusione fino a due anni e con la multa non inferiore a euro 1.000».

La condotta di detenzione assume quindi rilevanza autonoma: la disposizione, in virtù della clausola di sussidiarietà, trova applicazione solo nei casi in cui il soggetto agente non abbia realizzato le condotte prescritte all'art. 600 *ter* c.p., e, conseguentemente, viene esclusa la possibilità di concorso tra quest'ultima fattispecie e quella *de quo*. È stata la stessa Corte di Cassazione, dapprima nel 2017[116] e poi nel 2022[117], ad affermare che «non è configurabile il concorso tra il reato di detenzione di materiale pornografico di cui all'art. 600 *quater* c.p. ed il reato di distribuzione, divulgazione e diffusione di materiale pornografico di cui all'art. 600 *ter* c.p., comma 3, dovendo applicarsi, in virtù della clausola di riserva di cui all'art. 600 *quater* c.p., la più grave fattispecie di cui all'art. 600 *ter* c.p., a condizione che vi sia sovrapposizione o, comunque, tendenziale identità tra materiale detenuto e materiale divulgato; quando invece il primo sia talmente ingente da doversi escludere - con accertamento di fatto riservato al giudice del merito - che sia stato integralmente divulgato, la clausola di riserva non opera, poiché la condotta di detenzione si prospetta come autonoma ed ulteriore, sotto il profilo cronologico e naturalistico, ed è dotata di una carica di offensività propria rispetto alle condotte tipizzate dall'art. 600-ter c.p.».

[115] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 173.
[116] Cass., Sez. III, n. 20891/2017.
[117] Cass., Sez. III, n. 38178/2022.

La pronuncia delle Sezioni Unite del 2018[118] ha avuto un impatto anche con riferimento all'art. 600 *quater c.p.*: partendo dal presupposto che oggetto della norma de quo e quello dell'art. 600 *ter* è lo stesso materiale pedopornografico, il *diescrimen* tra le due fattispecie non può discendere dal pericolo concreto di diffusione. Conseguentemente, la distinzione discenderà dal fatto che il soggetto produttore del materiale coincida o meno con colui che lo detiene. Nel primo caso, in virtù della clausola di riserva contenuta al comma 1 dell'art. 600 *quater* c.p., troverà applicazione la fattispecie più grave contenuta all'art. 600 *ter* c.p., viceversa, in caso di soggetti detentori diversi, si applicherà l'art. 600 *quater* c.p[119].

La norma, a far datata dalla novella del 2006[120], ha ad oggetto una duplice condotta: quella di "procurare" e quella di "detenere". La prima fa riferimento ai casi in cui un soggetto si rivolge a un esercizio commerciale o a siti *internet* per procurarsi il materiale pedopornografico: in questo caso, quindi, il soggetto agente attua una condotta verso l'esterno, rivolta ai soggetti che hanno realizzato le condotte ex art. 600 *ter* c.p. La condotta di detenzione, invece, si risolve nel possesso del materiale pedopornografico, che può avvenire sia mediante un supporto "fisico", quindi tramite il salvataggio delle immagini su un dispositivo (come ad esempio un *hard disk)*, che per via telematica navigando in rete. In quest'ultimo caso, infatti, il soggetto che visiona le immagini su *internet* si trova in una situazione di immediata disponibilità e accessibilità del materiale[121], comportando un incremento della domanda di questo tipo di contenuto illecito[122] e quindi una lesione al bene tutelato dalla norma.

Il reato è punito a titolo di dolo diretto e, a differenza di ciò che si è detto con riguardo al comma 4 dell'art. 600 *ter* c.p., il legislatore ha mantenuto l'avverbio "consapevolmente", escludendo in questo modo la punibilità della condotta a titolo di dolo eventuale. Se non vi sono dubbi circa la rilevanza penale della condotta di colui che acquista consapevolmente da terzi, la stessa risulta, invece, esclusa nelle ipotesi in cui le immagini pedopornografiche risultino scaricate nel *pc* del soggetto senza che questo ne sia consapevole. In questo caso, infatti, non solo mancherebbe l'elemento soggettivo, ma ancor prima quello oggettivo consistente nella possibilità di disporre del materiale liberamente. Qualora il soggetto

[118] Cass., SS.UU., n. 51815/2018.
[119] ROMANO, *La pornografia minorile nella (nuova) lettura delle Sezioni Unite: dal pericolo concreto al reato di danno,* in *Cass. pen*., 2019, fasc. 2, p. 609.
[120] Prima della Legge n. 38/2006 il termine utilizzato era "disporre" e non "detenere".
[121] Cass., Sez. V, n. 36094/ 2006, in cui è stato ritenuto applicabile l'art. 600 *quate*r c,p. nel caso di un soggetto che teneva nascosto in un armadio un quaderno contenente materiale pedopornografico.
[122] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 155.

venisse a conoscenza dei *files* salvati sul proprio *pc* e ne prendesse visione, la cancellazione immediata del contenuto lo esenterebbe dal rispondere per detenzione[123].

La disposizione in analisi disciplina un reato commissivo permanente, la cui consumazione ha inizio nella fase di "procacciamento" del materiale e permane per tutto il tempo in cui il soggetto agente ha la disponibilità delle immagini[124].

Al comma 2, infine, è contenuta una circostanza aggravante relativa all'ingente quantità di materiale, per la valutazione della quale la Corte di Cassazione ha ritenuto opportuno imporre al giudice di «tener conto, oltre che al numero di supporti informatici detenuti, anche del numero di immagini che ciascuno contiene»[125].

### 2.3. La pornografia "virtuale".

L'art. 600 *quater 1* c.p. è stata una della novità introdotte con la Legge n. 38/2006, all'art.4, per ampliare il concetto di pedopornografia. L'articolo, stabilendo che: «Le disposizioni di cui agli articoli 600-ter e 600-quater c.p. 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», parifica[126] espressamente, per la prima volta, la pornografia realizzata mediante la tecnologia[127] e quella in cui viene materialmente usato un minore "in carne e ossa".

La disposizione è stata strutturata seguendo i modelli degli artt. 600 *ter* e *quater* c.p., motivo per il quale enuclea una fattispecie punita a titolo di dolo diretto, in relazione alla fattispecie di detenzione di materiale pedopornografico, e generico con riguardo a tutti gli altri casi[128].

---

[123] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 156 e SELLAROLI – LOMBARDO – GIRARDI, *Pedopornografia e reati in ambito sessuale, op. cit.,* p. 294.
[124] Cass., Sez. III, n. 22043/2010 e MANNA - RESTA, *I delitti in tema di pedopornografia, cit.,* p. 230.
[125] Cass., Sez. III, n. 39543/2017.
[126] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 144.
[127] Cass., Sez. III, n. 15757/2017: caso in cui è stata riconosciuta rilevanza penale di colui che ha prodotto materiale pedopornografico, mediante il programma grafico "Photoshop", realizzando un fotomontaggio in cui volti reali di mori erano stati sovrapposti a corpi di adulti impegnati in pratiche sessuali.
[128] CADOPPI, *Commento all'art. 600-quater.1 c.p.*, in *Commentario delle norme contro la violenza sessuale e la pedofilia*, a cura di CADOPPI, Padova, 2006, p. 282.

La *ratio* della fattispecie è quella di estendere l'operatività degli art. 600 *ter e quater* anche a quelle ipotesi in cui non vi sia stato un effettivo sfruttamento sessuale del minore, ma bensì un fotomontaggio di quest'ultimo in situazioni apparentemente reali. In questi casi, infatti, l'utilizzo dei programmi di elaborazione grafica è volto a far risultare indistinguibile il confine tra la realtà e il virtuale, così da «rendere verosimile una situazione insistente»[129].

Possono essere individuate tre diverse tipologie di pornografia virtuale[130]: i) "apparente", esclusa poi dalla norma, che si sostanzia in rappresentazioni di soggetti che richiamano esteticamente tratti adolescenziali[131]; ii) parzialmente virtuale che si risolve in fotomontaggi o *collage* in cui, ad esempio, si sovrappone il viso di un minore al corpo di un adulto ritratto in attività sessuali[132]; iii) integralmente virtuale in cui le immagini ritraenti minori sono una «pura elaborazione artificiale»[133].

Nonostante le diverse opinioni dottrinali[134], l'impostazione maggioritaria ha sempre ritenuto che l'art. 600 *quater 1* c.p. fosse un reato autonomo[135]. Ciò lo si può desumere, innanzitutto, dal fatto che il legislatore ha inserito la pornografia virtuale in un articolo separato e, in secondo luogo, dalla circostanza per cui, a differenza degli artt. 600 *ter* e *quater* c.p., l'oggetto della condotta sia si un minore, ma non in carne e ossa. Inoltre, se questa disposizione fosse stata pensata dal legislatore in termini di circostanza attenuante, sarebbe stato più logico e coerente inserire un nuovo comma all'art. 600 *sexies* c.p., piuttosto che integrare il codice con un nuovo articolo[136].

Inoltre, avendo l'art. 600 *quater 1* c.p. portata innovativa e non meramente ricognitiva di significati già esistenti, la Corte di Cassazione è intervenuta specificando l'esclusione dalla punibilità della fattispecie per tutti i fatti antecedenti rispetto all'entrata in vigore della stessa[137]. La *ratio* che sta alla base della normativa è, infatti, quella di impedire la crescita della domanda di materiale pedopornografico in favore della tutela del minore, andando però ad intaccare anche il profilo psicologico del pedofilo[138].

---

[129] PECCIOLI, *Un ulteriore intervento a tutela dei minori (I parte*), cit., p. 146.
[130] BIANCHI, *Commento all'art. 600-quater.1 c.p*., in *Commentario delle norme contro la violenza sessuale e la pedofilia*, a cura di CADOPPI, Padova, 2006, p. 243.
[131] Trib. Milano, Sez IX, n. 721/2010.
[132] BIANCHI, *Commento all'art. 600-quater.1 c.p*., op. cit., p. 243.
[133] MANNA - RESTA, *I delitti in tema di pedopornografia, cit.,* p. 231.
[134] CARINGELLA – DE PALMA – FARINI – TRINCI, op. cit, p. 1033 in cui, ad esempio, si ritiene che l'art. 600 *quater 1* c.p. non sia una fattispecie autonoma di reato, ma bensì una circostanza attenuante.
[135] BIANCHI, *Commento all'art. 600-quater.1 c.p*., op. cit., p. 266.
[136] BIANCHI, *Il "sexting minorile" non è più reato*?, in *Dir. pen. cont.*., 2016, fasc. 1, p. 138.
[137] Cass., Sez. III, n. 21631/2010.
[138] CADOPPI, *L'assenza delle cause di non punibilità mette a rischio le buone intenzioni*, in *Guida dir*., 2006, fasc. 9, p. 40, ha parlato in proposito di "guerra la nemico pedofilo", in cui l'oggetto della sanzione penale non sarebbe l'azione concreta posta in essere dal *reo*, quanto più la repressione di un "bruto" pensiero.

Nonostante dal dettato della norma risulti ovvio l'intento del legislatore di interdire la produzione di immagini mediante il ricorso a programmi avanzati e *ad hoc*, ma anche quelle prodotte con modalità più "artigianali"[139], poco chiaro risulta il confine della rilevanza penale rispetto a quelle immagini caratterizzate da "grossolanità". Si ritiene, però, che l'ultima parte del comma secondo[140] escluda la rilevanza penale ogni qual volta l'immagine, frutto dell'elaborazione informatica, non appaia reale[141].

Dall'altra parte, altrettanti dubbi interpretativi sono emersi con riguardo al grado di virtualità richiesto dalla norma. Abbracciando un'interpretazione restrittiva, l'operatività della stessa verrebbe circoscritta a quel materiale in cui si è fatto uso di immagini di minori reali o di parti riconoscibili di essi. In quest'ottica si ritiene ravvisabile una concreta lesione del bene giuridico, intesa come lesione della reputazione e sessualità del minore il cui volto è stato utilizzato[142]. In base a un'altra interpretazione, invece, si estenderebbe la rilevanza penale anche al materiale in cui il minore utilizzato non risulta riconoscibile[143]. Questa ricostruzione porterebbe, tuttavia, a un'esasperazione della norma anche in casi in cui non vi sia una concreta offesa al minore.

La Cassazione, nel 2017[144], è intervenuta in materia affermando la rilevanza penale non solo nel caso della pornografia parzialmente virtuale, ma anche in caso di virtualità totale. L'art. 600 *quater 1* c.p. è stato ritenuto applicabile anche nel caso di "fumetti pedopornografici". In quel caso la Corte ha affermato che «il bene protetto non debba essere considerato necessariamente, [...], la libertà sessuale del soggetto minore di età concretamente rappresentato e quindi, individuato, [...], da qualificare quale persona offesa; si è invece inclusa nella nozione di persona offesa dai reati in questione "i bambini e/o le bambine", da intendersi quale categoria di persone destinatarie della tutela rafforzata dell'intimità sessuale, incluso il rispetto delle diverse fasi del loro sviluppo fisico e psicologico, da intendere come comprensivo dello sviluppo della loro sessualità». Quindi, l'interesse oggetto di tutela sarebbe la sessualità dei minori, quale categoria di soggetti che non potrebbero esprimere un valido consenso. La Corte, pertanto, conclude ritenendo che risulta «superflua qualunque verifica circa il fatto che la condotta di rappresentazione

[139] Ad esempio, scannerizzare una foto di un minore e, sfruttando un'altra foto di un nudo, con il metodo "taglia- incolla", modificarla rendendola materiale pornografico.
[140] Si sta facendo riferimento all'inserto della norma che recita: «la cui qualità di rappresentazione fa apparire come vere situazioni non reali».
[141] DESISTO – DEZZANI – SANTORIELLO, *I reati di pedofilia informatica, op.cit.,* p. 145.
[142] BIANCHI, *Commento all'art. 600-quater.1 c.p*., op. cit., p. 263.
[143] Cass., Sez. III, n. 40748/2013 in cui la rappresentazione di parti del corpo di un infraquattordicenne, senza che compaia il volto di quest'ultimo, contenute in un telefonino rientrino nell'alveo dell'art. *600 quater 1* c.p.
[144] Cass., Sez. III, n. 22265/2017.

pedopornografica avesse offeso i minori specificatamente coinvolti nella rappresentazione, ossia risultasse concretamente diretta a danneggiare la loro libertà sessuale o personalità, ovvero che vi fosse stato un pericolo concreto per la personalità e sviluppo del minore rappresentato, essendo stata considerata dal legislatore la diffusione e la detenzione del materiale rappresentativo di minori implicati in attività di carattere sessuale, [...], non hanno, non solo per il nostro ordinamento ma per la comunità internazionale, quella maturità psicologica necessaria ad esprimere un valido consenso né alle attività sessuali in esse rappresentate ed ancor meno in tali rappresentazioni».

Quindi, il fatto di voler punire questo tipo di condotta trova la sua *ratio* nella tutela dello sviluppo del minore, cercando di impedire la "normalizzazione" delle interazioni sessuali tra adulti e minori e il conseguente impatto negativo che ciò avrebbe sulla collettività[145]. L'intento, tuttavia, deve essere perseguito senza portare a un'eccessiva applicazione dell'articolo con conseguenti risvolti pratici assurdi.

## 3. Il fenomeno del *Sexting* e la reazione della giurisprudenza.

Il termine "*Sexting*" si compone di due parole: "*sex*" e "*texting*". Con questa espressione si rimanda alla pratica di produzione e diffusione di «testi a sfondo sessuale ed esplicite immagini sessuali della propria persona, per mezzo di strumenti fotografici digitali, *webcam* o telefoni cellulari»[146]. Qualora il prodotto, oggetto di *sexting*, dovesse ritrarre un minore, si può parlare di materiale pedopornografico.

Trattasi di un fenomeno ormai dilagato in Italia e le cui vittime sono sempre più spesso adolescenti. Questi ultimi si ritrovano frequentemente a relazionarsi sui *social networks* e ciò che magari è iniziato come un gioco sessuale o di puro divertimento, come l'invio di immagini provocanti, può facilmente trasformarsi nell'incubo peggiore per un ragazzino in piena fase adolescenziale. Infatti, la sicurezza che ciò che viene inviato privatamente a un destinatario rimanga riservato non è mai assoluta e le conseguenze che, soprattutto a livello psicologico, possono derivare dalla diffusione di immagini private può essere devastante e addirittura portare a un «tragico epilogo»[147].

Tale fenomeno si è aggravato con l'evoluzione tecnologica e la conseguente entrata in gioco, a fianco dei semplici messaggi composti da parole, di materiali multimediali come

[145] BIANCHI, *I confini della repressione penale della pornografia minorile*, op. cit., p. 490.
[146] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 204.
[147] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 205.

*selfie*, video e foto. A partire dai dati emersi da uno studio attuato dal Telefono Azzurro nel 2019, è stata segnalata la presenza di una percentuale di pornografia domestica (anche detta *sexting*) pari al 22% tra la popolazione giovanile, sia maschile che femminile[148]. L'evoluzione tecnologica ha portato anche a un aumento degli utenti dell'*internet,* circostanza che ha spiegato l'aumento del 94% avvenuto tra il 2016 e il 2018 delle vittime dei reati contro la persona a sfondo sessuale. Inoltre, durante la pandemia da COVID- 19, la Polizia postale ha evidenziato non solo un incremento delle intrusioni nelle piattaforme destinate a uso didattico, ma anche della commissione dei reati a sfondo sessuale su minori[149]. Quindi, ad oggi, ciò che circola sul *web* non è solo il materiale pedopornografico etero- prodotto, con finalità di tipo commerciale, ma anche quello auto-prodotto da soggetti senza reale consapevolezza delle conseguenze delle proprie azioni.

Nonostante si tratti di un problema di una certa rilevanza, con presupposti differenti rispetto ai reati di pedopornografia virtuale e adescamento, il legislatore non ha ancora provveduto all'inserimento di una normativa contro il *sexting*. È stata la dottrina[150] a distinguere il fenomeno in due categorie. Da una parte vi è il *sexting* primario, che racchiude i casi di auto-produzione; quindi, le ipotesi in cui è lo stesso protagonista dell'immagine a inviarla a un diverso soggetto. Tendenzialmente, ciò si verifica nell'ambito di una relazione privata e con il consenso del soggetto ritratto nella foto. Dall'altra parte, il *sexting* secondario, invece, si sostanza nella divulgazione in rete o a diversi destinatari terzi dell'immagine pornografica che era stata prodotta con l'iniziale consenso del soggetto.

Dato ormai oggettivo è che spesso il diritto penale si presenta insufficiente davanti ai mutamenti sociali e culturali, presentando lacunosità che devono poi essere colmate dall'attività del giudice, quale interprete a tutela dei consociati. Questa dinamica si è verificata anche con riguardo al fenomeno del *sexting* portando la giurisprudenza a fare ricorso all'art. 600 *ter* c.p., in caso di pericolo concreto di diffusione, e all'art.600 *quater* c.p.[151]

Prima della pronuncia delle SS.UU del 2018 con riguardo alla natura dell'art. 600 *ter* c.p., la giurisprudenza, in linea con il *dictum* pronunciato nel 2000 con la sentenza Bove[152], era ferma nel ritenere necessaria la sussistenza del pericolo concreto di diffusione del

[148] Si trova sul sito https:// www.documentazione.info/telefono-azzurro-diffuso-il-dossier-2019-sugli-abusi
[149] Incremento del 110% di questa tipologia di reati, con 69 arresti e 1192 persone denunciate. Vedi il sito https:// www.commissariatodips.it/notizie/articolo/polizia-postale-e-delle-comunicazioni-e-tempo-di-bilanci.
[150] BIANCHI, *Il "sexting minorile" non è più reato*?, cit., p. 139.
[151] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 210.
[152] Cass., SS.UU., n. 13/2000.

materiale che il giudice avrebbe dovuto valutare in base a determinati indici sintomatici. Secondo questa ricostruzione si sarebbero dovute escludere dalla condotta di "produzione" le ipotesi di realizzazione autonoma di materiale pornografico ad uso strettamente privato[153]. Un passo avanti, però, si registrò nel momento in cui la giurisprudenza di legittimità iniziò a riconoscere la punibilità della pornografia domestica sulla base dell'art. 600 *quater* c.p.[154], consentendo così una tutela contro condotte caratterizzate da disvalore, anche se obiettivamente di diversa intensità rispetto a quelle rientranti nell'art. 600 *ter* c.p.

Una tesi dottrinale sviluppatasi prima della novella del 2006, invece, basava, la rilevanza penale della condotta sull'età della vittima: se è ultraquattordicenne era necessario il pericolo concreto di diffusione, diversamente l'offensività era *in re ipsa*[155].

Rilevante in materia è la sentenza n. 163 del 2015, emessa dal Tribunale di Firenze. Il caso di specie riguardava una ragazza quasi maggiorenne e un ragazzo maggiorenne impegnati in una relazione sentimentale, che durante la frequentazione erano avvezzi a registrare consensualmente video dei propri rapporti sessuali e detenerli nel dispositivo della ragazza, eccetto per un unico video. Al termine della relazione, il ragazzo aveva pubblicato quest'ultimo su *Facebook* e, a seguito di querela, era stato sottoposto a processo per i reati di cui agli artt. 600 *ter* comma 1 c.p. e 600 *ter* comma 3 c.p. Il GIP assolse l'imputato per il reato di produzione "perché il fatto non sussiste" e lo condannò, invece, per quello di divulgazione. In *primis,* il giudice, oltre a sottolineare come l'obiettivo principale della normativa fosse quello di tutela del minore di fronte a "ogni tipo di abuso sessuale", richiamò la giurisprudenza delle SS.UU del 2000, sostenendo la natura di reato di pericolo concreto dell'art. 600 *ter* c.p. Nel fare poi un'analisi ermeneutica della norma, si soffermò sul termine "utilizzare" affermando che «l'utilizzazione del minore può ritenersi integrata ogniqualvolta lo stesso risulti destinatario di condotte o di atti tali da ritenersi corrispondenti ai poteri comunemente esercitati sulle cose, che in conseguenza rendono la condizione del minore equiparabile a quella della schiavitù»[156]. Nel valutare questo elemento, il giudice ha ritenuto imprescindibile il fatto di non escludere la valenza del consenso in base alla distinzione dell'età della vittima, in linea con la dottrina minoritaria predetta: il consenso non rileva se la vittima è infra-quattordicenne, mentre, qualora si tratti di un soggetto ultraquattordicenne, la libertà, spontaneità e consapevolezza del consenso dovranno essere accertate dal

[153] BIANCHI, *I confini della repressione penale della pornografia minorile*, *op. cit*., p. 135.
[154] Cass., Sez. III, n. 11997/ 2011.
[155] CADOPPI, *Commento art. 600-ter I e II comma c.p., in Commentario delle norme contro la violenza sessuale e contro la pedofilia*, *op.cit*, p. 149.
[156] Trib. Firenze, n. 163/2015.

giudice[157]. In seguito, affermando che «in presenza di un tale consenso, che sia validamente prestato secondo le condizioni sopra indicate, ritenere che lo stesso non abbia alcun valore nella valutazione del caso concreto, potrebbe in ipotesi limitare fortemente quella stessa libertà sessuale, e le relative manifestazioni della stessa, che l'ordinamento invece vuole riconoscere»[158], il giudicante ha concluso nel senso di non ravvisare l'elemento dell'"utilizzazione", assolvendo quindi l'imputato con riguardo al reato di produzione di materiale pornografico.

Con riguardo, invece, al secondo capo di imputazione, il giudice ha operato un'interpretazione che può ritenersi senza dubbio forzata. In particolare, nella motivazione non viene tenuto conto del rinvio operato dal legislatore nei commi successivi al primo dell'art. 600 *ter* c.p., in base al quale il materiale pedo-pornografico deve essere quello "di cui al primo comma" della stessa norma, proponendo quindi una scissione tra la condotta punita al comma 1 e le successive[159]. In questo senso, quindi, il giudice, ritenuto il video caricato su *Facebook* conforme alla definizione di materiale pedopornografico, ha affermato la punibilità della divulgazione, anche in assenza dell'utilizzazione della minore[160].

Successivamente, la Corte di Cassazione è intervenuta sul tema con la sentenza n. 11675/2016. Il caso di specie riguardava una minorenne che, dopo aver realizzato degli auto-scatti pornografici, li inviava a un gruppo di amici, i quali poi li cedevano a terzi, ad eccezione di un amico che, invece li aveva tenuti per sé.

Il Tribunale per i minorenni dell'Abruzzo aveva proceduto, da una parte, nei confronti di quest'ultimo sulla base dell'art. 600 *quater* c.p., e, dall'altra, nei confronti degli altri amici ai sensi dell'art. 600 *ter*, comma 4 c.p. Il giudicante concluse affermando di non doversi procedere per insussistenza del fatto. A risposta, il Procuratore della Repubblica propose ricorso in Cassazione, facendo leva sul rischio di un pericoloso vuoto di tutela, contro coloro che furono imputati per cessione di materiale pedopornografico. Il ricorso venne successivamente respinto a favore dell'interpretazione avanzata in primo grado: sostanzialmente, la Corte affermando la necessarietà, ai fini della configurabilità dell'art. 600 *ter* c.p., del requisito di "alterità e diversità" tra il soggetto produttore del materiale e di

[157] BIANCHI, *I confini della repressione penale della pornografia minorile*, op. cit., p. 169.
[158] Trib. Firenze, n. 163/2015.
[159] BIANCHI, *Ibidem,* in base al quale l'interprete è chiamato a valutare solamente le caratteristiche delle immagini e gli elementi della condotta, a prescindere dal modo in cui l'immagine sia stata realizzata e quale sia stato il consenso.
[160] BIANCHI, *Ivi.,* p. 170.

colui che ne è oggetto, escluse la rilevanza penale dei cosiddetti *selfies*[161]. Questa ricostruzione aveva l'obiettivo di scongiurare una rischiosa, nonché inammissibile, analogia in *malam partem*[162].

La Corte, in accordo con il Tribunale per i minorenni dell'Abruzzo, partiva dall'elemento letterale dell'"utilizzazione", inteso quale "utilizzo strumentale del minore", in linea con il principio di diritto affermato con la Sentenza Bove, facendone derivare il presupposto logico in virtù del quale l'utilizzazione, e di conseguenza la produzione, sono condotte che devono essere realizzate da un soggetto diverso rispetto al minore utilizzato. Qualora dovesse venire a mancare questo requisito, l'art. 600 *ter* c.p. non potrebbe trovare applicazione per assenza di un elemento costitutivo. Inoltre, fondamentale per questo approdo giurisprudenziale è stato il rinvio, presente all'art. 600 t*er* c.p., «al materiale pornografico di cui al comma 1», in base al quale la Corte ha ritenuto non punibili le condotte di cessione, divulgazione e diffusione qualora non abbiano ad oggetto materiale prodotto da terzi utilizzando un minore di 18 anni[163].

Nel caso di specie, la Corte ha ritenuto non configurabile l'art. 600 *ter*, comma 4 c.p. per difetto del requisito di "alterità e diversità" tra soggetto produttore e oggetto dell'immagine, trattandosi di immagini prodotte in modo autonomo e consapevole dalla minore stessa.

A differenza della precedente pronuncia analizzata, in questa sentenza non si tocca il tema del consenso se non in un *obiter dictum* in cui si legge che il consenso del minore è «del tutto irrilevante»[164]. Tuttavia, se da una parte è chiara l'esclusione della rilevanza penale della pornografia domestica per difetto di un elemento costitutivo, dall'altra, le condotte di *sexting* si possono manifestare nei modi più disparati (ad esempio, nel caso affrontato dal Tribunale di Firenze il video incriminato era stato girato sia dalla vittima che dall'*ex* fidanzato) e ciò evidenzia il *deficit* che caratterizza un'interpretazione che escluda il valore del consenso[165].

Il pregio di questa sentenza, che l'accomuna con quella precedente, è quello di mettere in luce la difficoltà del diritto penale a adattarsi e contrastare il nuovo fenomeno del *sexting*,

---

[161] BIANCHI, *Ivi.,* p. 171, definisce i *selfies* come «auto-scatti effettuati dallo stesso minore immortalato nell'immagine».
[162] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 215.
[163] Cass., Sez. III, n. 11675/2016.
[164] Cass., Sez. III, n. 11675/2016.
[165] BIANCHI, *I confini della repressione penale della pornografia minorile*, *op. cit*., p. 175.

che si presenta come qualcosa di diverso rispetto alle condotte che inizialmente il legislatore mirava a contrastare[166].

Con il tempo e il progresso tecnologico, la giurisprudenza si è ritrovata a dover fare i conti con l'intrinseca pericolosità diffusiva che caratterizza i *social networks* e a dover rivisitare, quindi, l'orientamento precedente.

Con la pronuncia delle SS.UU del 2018, n. 51815, la Corte ha attuato il primo passo avanti verso la rilevanza penale della pornografia domestica. Infatti, chiarendo il significato del termine "utilizzazione", ossia strumentalizzazione del minore[167], si è affermata non solo la natura di reato di danno dell'art. 600 *ter* c.p., ma anche la punibilità di questo fenomeno quando il materiale venga «prodotto in maniera abusiva mediante la strumentalizzazione del minore»[168].

Questa sentenza è stata fondamentale anche con riguardo la tema del consenso: se per i minori di quattordici anni l'abusività della produzione domestica è *in re ipsa*; in caso di minori tra i quattordici e i diciotto anni, l'abusività della produzione dipende dalla posizione dominante assunta dal soggetto agente. Detto diversamente, le condotte rientrano nel termine "utilizzazione" sono quelle riconducibili a «una posizione di supremazia (…) o per le modalità con le quali il materiale pornografico viene prodotto (ad esempio, minaccia, inganno) o per il fine commerciale (…) o per l'età dei minori coinvolti, qualora questa sia inferiore a quella del consenso sessuale»[169]. In questo senso, quindi, viene esclusa la rilevanza penale nei casi in cui l'immagine venga prodotta in modo consapevole e al fine di un uso strettamente personale[170]. Ciò che fa venir meno l'illiceità della condotta, infatti, non è tanto il consenso di per sé, quanto piuttosto il contesto in cui esso è stato eventualmente prestato, per cui sarebbe certamente invalido in presenza di questo tipo di utilizzo del minore[171].

La giurisprudenza successiva alla sentenza del 2018 ha confermato sia il venir meno del pericolo concreto di diffusione che la punibilità della pornografia domestica ai sensi dell'art. 600 *ter* comma 1 c.p. Tuttavia, sono rimasti aperti dubbi interpretativi che hanno portato le Sezioni Unite a pronunciarsi nuovamente con la sentenza n. 4616 del 2022.

---

[166] BIANCHI, *Ibidem.*
[167] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 218, definisce il termine come «la trasformazione del minore, da soggetto dotato di libertà e dignità sessuali, in strumento per il soddisfacimento di desideri sessuali di altri o per il conseguimento di utilità di vario genere».
[168] PECCIOLI, *La rilevanza penale della pedopornografia ad uso personale tra punti fermi e residui profili critici,* in Dir. pen. proc., 2022, fasc. 9, p. 1199.
[169] Cass., S.U., n. 51815/2018.
[170] PECCIOLI, *Ibidem.*
[171] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 218.

Il considerato in diritto si apre con un *excursus* storico dell'art. 600 *ter* c.p. la menzione delle relative interpretazioni che si sono succedute sino al 2018 e delle esigenze di adeguamento agli obblighi internazionali. Viene, poi affermato, richiamando espressamente un passaggio della sentenza del 2018, che «il discrimine fra il penalmente rilevante e il penalmente irrilevante… non è il consenso del minore in quanto tale, ma la configurabilità dell'utilizzazione»[172]. Così facendo, la Corte evidenzia come la punibilità della pornografia domestica e delle altre condotte discenda dall'esistenza di un abuso di una posizione dominante, da verificare in modo puntuale[173], la quale renderebbe invalido il consenso.

Ancora, il consenso inizialmente dato con riguardo al rapporto sessuale non si estende all'eventuale successiva registrazione dell'atto e divulgazione che, invece, rappresentano nuove condotte abusive lesive dell'art. 600 *ter* c.p.[174].

È stato precisato, inoltre, che qualora il minore venga indotto o istigato ad auto-produrre delle immagini pornografiche, queste due condotte di istigazione e induzione realizzate dal soggetto agente rientrerebbero nel concetto di "utilizzazione". Infatti, portare un minore a realizzare delle fotografie provocanti o far sorgere in lui il proposito a farlo, presenta il medesimo disvalore offensivo che caratterizzerebbe un classico caso di produzione di materiale pornografico, meritevole quindi di tutela ai sensi dell'art. 600 *ter* c.p.[175].

La seconda parte della sentenza si concentra, invece, sui rapporti che intercorrono tra il comma 1 e i successivi commi 2, 3 e 4 dell'art. 600 *ter* c.p.

La Corte, prima di tutto, nel richiamare la precedente sentenza della Sezione III, n. 5522/2019, precisa che con il rinvio presente ai commi 2, 3 e 4 dell'art. 600 *ter* c.p. «al materiale di cui al primo comma» si sta facendo riferimento «non all'intera condotta delittuosa del primo comma, ma all'oggetto materiale del reato»[176], risultando quindi «necessario e sufficiente che oggetto dell'offerta o della cessione sia il materiale pedopornografico realizzato o prodotto»[177]. Di conseguenza, ciò che rileva saranno le caratteristiche di quest'ultimo e il fatto che rientri nella nozione di materiale pornografico contenuta al comma 7[178].

---

[172] Cass., S.U, n. 51815/2018, richiamata a p. 12 della sentenza n. 4616/2022.
[173] Cass., S.U, n. 4616/2022, p. 22, si legge espressamente il seguente principio: «si ha "utilizzazione" del minore allorquando, all'esito di un accertamento complessivo che tenga conto del contesto di riferimento, dell'età, maturità, esperienza, stato di dipendenza del minore di, si a Parisi no forme di coercizione o di condizionamento della volontà del minore stesso, restando escluse dalla rilevanza penale solo condotte realmente prive di offensività rispetto all'integrità psicofisica dello stesso».
[174] Cass., S.U, n. 4616/2022, p. 20.
[175] PECCIOLI, *La rilevanza penale della pedopornografia ad uso,* cit., p. 1200.
[176] Cass., Sez. III, n. 5522/2019.
[177] Cass., Sez. III, n. 5522/2019.
[178] Cass., S.U, n. 4616/2022, p. 23.

Fatta questa premessa, la Corte affronta il vero dubbio interpretativo: «se anche il materiale "autoprodotto" dal minore possa essere ricompreso nelle fattispecie dei commi terzo e quarto per effetto del richiamo "al materiale del primo comma"»[179].

Partendo dal dato oggettivo in base al quale il materiale pornografico deve rimanere nella sfera privata dei soggetti coinvolti per essere considerato "pornografia domestica", al venir meno di questo presupposto e, quindi, con la messa in circolazione di detto materiale, il minore viene strumentalizzato all'atto della cessione o diffusione. Conseguentemente, qualora la messa in circolazione sia contestuale o, ancora, rappresenti oggetto di una volontà presente fin dall'inizio nella mente del soggetto agente, allora quest'ultimo sarà punibile ai sensi del comma 1 dell'art. 600 *ter* c.p. Se, invece, la messa in circolazione fosse successiva alla produzione, allora troveranno applicazione i commi successivi al primo[180]. Questa seconda ricostruzione, condivisa in dottrina[181], si basa sulla considerazione che l'art. 600 *ter* c.p. sia stato volutamente strutturato seguendo una scala di disvalore, subordinando l'applicazione di un comma alla circostanza che la fattispecie non integri il comma precedente. La prima, invece, non pare esente da perplessità. Infatti, porre sullo stesso livello la produzione a fini domestici e quella a fini divulgativi pare irragionevole, vista l'evidente sproporzione sanzionatoria[182].

Per quanto concerne il consenso, la Corte afferma che questo non vale come esimente con riguardo alla condotta di divulgazione, ritenendo, infatti, che il minore «non può mai prestare validamente consenso alla circolazione del materiale realizzato (…) in quanto soggetto che presuntivamente non ha ancora raggiunto quel livello di maturità tale da consentirgli una valutazione davvero consapevole in ordine alle ricadute negative della mercificazione del suo corpo attraverso la divulgazione delle immagini erotiche»[183]. Ciò sulla base della considerazione che il bene tutelato non sia solo l'interesse individuale del singolo minore ritratto nell'immagine, ma anche quello collettivo di tutti i minori.

Dall'analisi di quest'ultima pronuncia, nonché dal complesso di questa parte di elaborato, risulta palese lo sforzo realizzato dalla giurisprudenza, ma al tempo stesso il suo insuccesso a causa dell'assenza di adeguati strumenti, nel far fronte al fenomeno della pornografia domestica[184], manifestando contemporaneamente l'urgenza di un intervento di

[179] Cass., S.U, n. 4616/2022, p. 23.
[180] Cass., S.U, n. 4616/2022, p. 24.
[181] PECCIOLI, *La rilevanza penale della pedopornografia ad uso,* cit., p. 1201.
[182] PECCIOLI, *Ibidem.*
[183] Cass., S.U, n. 4616/2022, p. 25.
[184] BIANCHI, *I confini della repressione penale della pornografia minorile*, *op. cit*., p. 175.

rivisitazione del legislatore dell'art. 600 *ter* c.p. che abbia ad oggetto il tema della pornografia ad uso personale[185].

### 3.1. L' *iter* che ha portato alla criminalizzazione del *Revenge porn* (*ex* art 612 *ter* c.p).

Lo sviluppo tecnologico, con l'emersione di nuovi strumenti tecnologici come *smartphone* dotati di fotocamera o *tablet,* e il continuo progresso che ha riguardato i *social media,* hanno reso il cyberspazio un luogo in cui la possibilità di pubblicare e condividere momenti della propria vita quotidiana si è risolto in un semplice *click* sullo schermo[186]. Se da un lato il progresso ha facilitato molti aspetti della vita dei consociati, dall'altro ha reso lo strumento tecnologico una possibile arma contro gli stessi. A titolo di esempio, prima la volontà di registrare un atto intimo doveva necessariamente essere seguita da una pluralità di condotte generalmente costose, come procurarsi una videocamera di una certa dimensione ed estrarre il video per poi elaborarlo[187]. Oggi, invece, è possibile registrare e pubblicare contenuti della vita privata in modo istantaneo, tramite *"post"*, se non addirittura simultaneo con le cosiddette *"lives"*, potendo raggiungere in un breve lasso di tempo innumerevoli *accounts,* anche localizzati all'estero, come avviene su determinate piattaforme (*Instagram, TikTok* e *Facebook*). Questo ha portato a un ampliamento della potenzialità offensiva di determinate azioni criminose e a un'inadeguatezza del diritto penale di fronte a nuove manifestazioni criminose[188].

Il continuo intrecciarsi tra tecnologia e pornografia ha portato all'emersione di nuove terminologie. Come si è già visto, si è iniziato a parlare di *Sexting,* nella sua duplice declinazione, primario e secondario, fino ad arrivare alla sua versione "degenerativa"[189], conosciuta comunemente come "*Revenge porn*". Questo fenomeno consiste, in senso stretto, nella creazione consensuale di immagini o video a sfondo sessuale, tendenzialmente nell'ambito di una relazione intima, e nella non consensuale pubblicazione degli stessi a scopo ritorsivo[190]. In realtà, il termine ha una capacità comprensiva molto più ampia: infatti,

---

[185] PECCIOLI, *La rilevanza penale della pedopornografia ad uso,* cit., p. 1201.
[186] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p.*, in *Dir. fam*., 2021, fasc. 3, p. 1431.
[187] Un esempio è il caso David Feltmeyer avvenuto nel 2007 a Chesterfield (USA), il quale, in assenza dei *social media* come sono sviluppati oggi, distribuì *dvd* con registrazioni di momenti intimi con la precedente *partner*.
[188] AMORE, *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.,* in *Leg. pen*., 2020, p. 4.
[189] COTELLI, *Pornografia domestica, sexting e revenge porn fra minorenni. Alcune osservazioni dopo la pronuncia delle Sezioni Unite n. 51815/18*., in *Giur. pen*., 2019, fasc. 3, p. 5.
[190] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 229.

nella sua accezione più ampia, ricomprende anche fattispecie lontane da ciò che si può definire come "porno-vendetta"[191]. Nell'ampio spettro di condotte che vengono generalmente racchiuse in questo concetto troviamo, ad esempio, il "*Deep sex fakes*", il "*Vouyerismo digitale*" o, ancora, la "pornografia estrema"[192]. Si può notare, quindi, come si possano presentare casi in cui il fine ultimo della condotta non è la vendetta, ma solo la volontà di degradare la vittima o di raggiungere un appagamento sessuale, oppure scenari in cui, addirittura, non vi è alcun tipo di legame sentimentale tra l'autore del reato e la vittima. Ciò che però sembra accomunare queste ipotesi è la diffusione non consensuale del materiale[193] e quindi la lesione della riservatezza della vittima, la quale viene ridotta a strumento per il soddisfacimento del soggetto agente.

Nella dottrina inglese[194] si è evidenziato come la questione terminologica abbia portato a ricostruzioni interpretative sfavorevoli alla vittima di *revenge porn.* Infatti, l'utilizzo del termine "*revenge*" enfatizza il motivo per il quale il soggetto agente può aver deciso di diffondere il materiale intimo: l'attenzione viene spostata sulla circostanza in base alla quale questa condotta è conseguenza di un torto precedentemente subito, come se questo ne giustificasse la gravità. Questa logica impatta negativamente sulla vittima, nell'ambito del cosiddetto "*victim blaming*"[195], soprattutto viste le conseguenze devastanti che quest'ultima si ritroverà a gestire[196]. Il termine "*porn*", inoltre, attribuisce all'atto un'accezione erotica, ma allo stesso tempo anche una sensazione di scelta, di "giusto"[197]. Questo, infatti, è un aggettivo che rimanda a immagini sessualmente esplicite volte ad appagare l'eccitazione altrui, intenzione che non caratterizza propriamente la condotta di diffusione illecita di

[191] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, op. cit., p. 6.
[192] Secondo AMORE, *Ibidem*, il primo termine fa riferimento a «rappresentazioni di rapporti sessuali alterate – in genere – per farvi apparire coinvolta una persona diversa da quella che lo ha effettivamente compiuto»; il secondo al caso di colui che «filma surrettiziamente le parti intime delle sue vittime, con la possibilità di diffondere in seguito le riproduzioni realizzate nei canali frequentati da coloro che si giovano di simili rappresentazioni»; la terza espressione, invece, indica quelle ipotesi in cui il consenso non vi è stato neppure per l'atto sessuale che viene ripreso.
[193] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p.*, op. cit., p. 1430.
[194] CITRON- FRANKS, *"Criminalizing Revenge Porn",* in *Wake Forest Law Review*, 2014, p. 345.
[195] In ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p., op. cit*., p. 1429, viene utilizzata quest'espressione per indicare quella tendenza della società a condannare e criticare la donna per aver deciso di inviare immagini intime di sé stessa.
[196] Come ad esempio, crisi d'ansia, depressione, perdita di auto-stima, sviluppo di un disturbo post-traumatico da stress e, in certi casi, della volontà di porre fine alla propria vita.
[197] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, op. cit., p. 9 e, nello stesso senso, CALETTI, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale,* in *Riv. it. dir. proc. pen.,* 2019, fasc. 3, p. 2054.

immagini pornografiche. Anzi, in questo caso vi è la consapevolezza e volontà dell'autore di arrecare un danno alla vittima oggetto delle immagini[198].

Da questa prospettiva, l'espressione "*revenge porn*" risulta impropria e ha portato la dottrina angloamericana a proporre alternative terminologiche più neutre come, ad esempio, "*non-consensual pornography*"[199].

Anche in Italia, quando si è deciso di inserire una norma *ad hoc* che contrastasse questo fenomeno, si è optato per un'espressione, ossia "diffusione illecita di immagini o video sessualmente espliciti", abbastanza ampia e neutra così da riuscire ad attrarre nel concetto plurime condotte, ma senza stigmatizzare la vittima, sottolineando l'assenza di un assenso di quest'ultima.

Vista la rilevante casistica e la risonanza di certi fatti di cronaca[200], si è sentita la forte esigenza di modificare l'ordinamento penale di modo da contrastare un fenomeno che, come emerso da certi studi[201], ha mostrato la sua elevata potenzialità offensiva, vista la viralità[202] che lo caratterizza. La reazione del nostro legislatore si è risolta nell'introduzione del nuovo art. 612 *ter* c.p., rubricato "Diffusione illecita di immagini o video sessualmente espliciti", con la Legge del 19 luglio 2019, n. 69 contenente le "Modifiche al Codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere" (cd. Codice rosso).

---

[198] LO MONTE, *il c.d. revenge porn nel contesto del 'codice rosso': i limiti della ricostruzione come subspecies della 'violenza di genere'*, in *Iura & Legal system*, 2021, fasc. 1, p. 115.

[199] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p.*, op. cit., p. 1429.

[200] Come, a titolo di esempio, il caso di Tiziana Cantone. A riguardo si veda CALETTI, *"Revenge porn" e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane*, in *Dir. pen. cont*., 2018, fasc. 3, p. 65.

[201] Ad esempio, come si legge in CALETTI, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensual, cit.,* p. 2056, il "*Sexual Assault Support Service*" ha condotto delle indagini con riguardo alle conseguenze sulle vittime derivanti da attacco da *revenge porn*, dal quale emerge che le reazioni più frequenti sono: sensazioni di vergogna, umiliazione, violazione personale ed impotenza; apprensione circa la propria sicurezza personale; percezione di essere costantemente sotto sorveglianza; paura di essere filmati durante le attività sessuali e tante altre. Ancora, nel 2020 è stato dato avvio a delle indagini con riguardo all'esistenza di plurimi gruppi *Telegram*, in cui numerosi utenti si scambiavano immagini e video pornografici, anche aventi ad oggetto minori. A riguardo si veda il sito https://www.wired.it/internet/web/2020/11/25/telegram-revenge-porn-gruppi-italia/. Addirittura, come evidenziato da CALETTI, *Ivi.,* p. 2055, ci sono dei casi in cui gli artefici di queste condotte, oltre a pubblicare il video intimo su una piattaforma *social*, inseriscono delle informazioni personali della vittima, aggravando ulteriormente le ripercussioni dell'azione su di essa.

[202] In CALETTI, *"Revenge porn" e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane*, cit., p. 80, si parla di incontrollabilità e inarrestabilità della diffusione delle immagini. Ad esempio, nel caso di Tiziana Cantone, il video pubblicato su *YouTube* aveva raggiunto più di 20 milioni di visualizzazioni, senza contare la diffusione dello stesso video in altre due piattaforme, quali *Facebook* e *WhatsApp.*

Prima dell'entrata in vigore della suddetta legge, i giudici si trovano a dover far fronte al fenomeno del *revenge porn* ricorrendo alle norme presenti nel Codice nella loro veste di interpreti, e così da supplire ad eventuali vuoti normativi. In questo senso, spesso si ricorreva all'applicazione dell'art. 595 c.p. (reato di diffamazione)[203], in particolare, nella sua forma aggravata ex co. 3, in quanto arrecata "col mezzo della stampa o con qualsiasi altro mezzo di pubblicità". Tuttavia, il ricorso a questa disposizione, sebbene sia stata utile per contrastare determinate ipotesi di *revenge porn*, non è risultata confacente alle esigenze di tutela. Infatti, come emerge dal comma 1 della norma, questa mira a contrastare condotte che incentrano il proprio disvalore sulla lesione alla reputazione della vittima. Invece, nei casi di *revenge porn*, ciò che viene leso non è solo la reputazione e l'onore[204], ma bensì la riservatezza e la fiducia che la vittima riponeva nell'autore della condotta, intaccando anche la libertà sessuale della prima[205]. Inoltre, l'inciso «comunicando con più persone» porta, sul piano applicativo, ad escludere tutte quelle ipotesi in cui l'invio dell'immagine abbia riguardato una relazione a due, senza garantire quindi una sufficiente tutela alla vittima che, ad esempio, abbia perso la propria posizione lavorativa a seguito dell'invio, da parte di terzi, di una foto intima al proprio datore di lavoro[206].

Tutto ciò evidenzia l'inadeguatezza dell'art. 595 c.p. nella la lotta contro il *revenge porn*.

Un'altra disposizione chiamata in causa dagli interpreti per arginare il fenomeno era l'art. 617 *septies* c.p. (diffusione di riprese e registrazioni fraudolente)[207]. Anche in questo caso, nonostante gli sforzi interpretativi, la normativa non è risultata adeguata a garantire una sufficiente tutela alle vittime di *revenge porn*[208]. *In primis*, la norma, con l'espressione "fraudolentemente", limita il proprio ambito di applicazione ai soli casi in cui non vi sia stato consenso da parte della vittima, escludendo quindi il materiale autoprodotto[209]. In secondo luogo, il fatto che gli incontri avvengano alla "presenza" o "partecipazione" di chi li ha ripresi portano ad escludere la punibilità, ai sensi di questa norma, di quei casi in cui l'autore

[203] L'articolo punisce: «Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a milletrentadue euro».
[204] Secondo CALETTI, *"Revenge porn" e tutela penale, cit.,* p. 83, questi sono beni che subiscono un'offesa incidentale rispetto a quella della riservatezza.
[205] BIANCHI, *Il "sexting minorile" non è più reato*?, cit., p. 153.
[206] CALETTI, *"Revenge porn" e tutela penale, cit.,* p. 83.
[207] L'articolo punisce: «Chiunque, al fine di recare danno all'altrui reputazione o immagine, diffonde con qualsiasi mezzo riprese audio o video, compiute fraudolentemente, di incontri privati o registrazioni, pur esse fraudolente, di conversazioni, anche telefoniche o telematiche, svolte in sua presenza o con la sua partecipazione, è punito con la reclusione fino a quattro anni».
[208] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit.,* p. 15.
[209] CALETTI, *"Revenge porn" e tutela penale, cit.,* p. 84.

non abbia preso parte all'incontro sessuale[210]; infine, essendo questo un reato a dolo specifico, come di deduce dall'inciso "al fine di recare danno all'altrui reputazione o immagine", i casi in cui l'intenzione dell'autore non fosse quella di ledere la reputazione della vittima, ma, ad esempio, solo quella di divertirsi[211], non troverebbero tutela alcuna.

Anche l'art. 600 *ter*, comma 3 e 4, c.p. avrebbe potuto trovare applicazione per le condotte oggetto di analisi, ma solo con riguardo a materiale pedopornografico[212]. Questa fattispecie, per altro, può trovare applicazione anche a seguito dell'entrata in vigore dell'art. 612 *ter* c.p[213].

Questi sono solo tre esempi di quelli che sono stati i tentativi degli interpreti[214] per fronteggiare il nuovo fenomeno del *revenge porn* in assenza di una norma *ad hoc.* Per due ordini di motivi nessuno è risultato idoneo a supplire alla lacuna normativa preesistente al 2019[215]: innanzitutto, essendo il *reveng porn* un fenomeno che si compone di una elevata varietà di condotte, il precedente impianto penale non garantiva una tutela omnicomprensiva di tutte queste varianti; infine, nessuna di queste disposizioni era in grado di tutelare la riservatezza e la libertà di autodeterminazione sessuale della vittima, ma solo un bene giudico specifico che rappresenta un interesse intaccato per vie incidentali dalle condotte di diffusione illecita di immagini e video pornografici[216].

### 3.1.1. La struttura dell'art. 612 *ter* c.p.

Come già preannunciato, con la Legge n. 69/2019 (Codice rosso), è stato dato ingresso nel nostro impianto penale al nuovo art. 612 *ter* c.p. Il Codice rosso ha rappresentato una risposta a diverse sollecitazioni sovranazionali, tra cui la Convenzione di Istanbul del 2011 sulla prevenzione e lotta contro la violenza sulle donne e la Direttiva 2012/29/UE adottata

[210] Un esempio è il caso di colui che filma di nascosto, dalla propria abitazione, una donna nuda.
[211] CALETTI, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale, cit.,* p. 2053.
[212] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, op. cit., p. 16.
[213] Secondo GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 236, l'art. 600 *ter* c.p., nel prevedere una pena più grave rispetto all'art. 612 *ter* c.p., dovrebbe poter "assorbire" il disvalore di quest'ultimo.
[214] In COTELLI, *Pornografia domestica, sexting e revenge porn fra minorenni, cit.,* p. 15, si legge espressamente che «talora, il *revenge porn* può essere ricondotto nell'ambito applicativo della diffamazione aggravata a mezzo di pubblicità, oppure della minaccia, della violenza privata o, nei casi più gravi, dell'estorsione (cd. fenomeno del *sextortion*). Non può essere ravvisato, invece, il reato di interferenze illecite nella vita privata».
[215] COTELLI*, Ibidem.*
[216] COTELLI*, Ibidem.*

con lo scopo di istituire un livello minimo di tutela per i diritti, assistenza e protezione delle vittime[217].

L'art. 612 *ter* c.p.[218] è un delitto comune, plurioffensivo[219], a condotta vincolata, di applicazione sussidiaria, vista la presenza della clausola di riserva[220]. La disposizione punisce, ai primi due commi, la stessa condotta di messa in circolazione non consensuale di immagini o video intimi, con il medesimo trattamento sanzionatorio[221] , distinguendo però il punto d'origine della condotta. Infatti, al comma 1 si inserisce, quale presupposto del reato, la "realizzazione" o l'"indebito impossessamento"[222] delle immagini o video poi diffusi, mentre, al comma 2 si fa riferimento ai cosiddetti distributori secondari, ossia coloro che abbiano ricevuto o acquisito in qualunque maniera il materiale pornografico e lo abbiano a loro volta diffuso[223]. Un'altra distinzione tra questi due commi è data dalla presenza, solo al comma 2, dell'inciso «al fine di recare loro nocumento» quale indicatore di una punibilità a titolo di dolo specifico. La dottrina[224] ha ritenuto non del tutto condivisibile la scelta di punire, solo limitatamente ai casi in cui l'autore si faccia carico di una volontà specifica, quelle condotte di distribuzione "ulteriore" avvenute a distanza di tempo e, probabilmente, da parte di soggetti "lontani" rispetto alla persona offesa. Infatti, se da un lato l'economia processuale ringrazia il legislatore, dall'altro, nel *mare magnum* di ipotesi che si possono verificare non sempre la finalità del distributore è quella di recare nocumento alla vittima:

---

[217] LO MONTE*, il c.d. revenge porn nel contesto del 'codice rosso': i limiti della ricostruzione come subspecies della 'violenza di genere'*, in *Iura & Legal system*, *op. cit*., p. 109.

[218] L'articolo recita: «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 reclusione 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. La remissione della querela può essere soltanto processuale. Si procede tuttavia d'ufficio nei casi di cui al quarto comma, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio».

[219] Secondo GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 229, è un reato diretto a tutelare sia la libertà di autodeterminazione sessuale, che la riservatezza, il decoro e la reputazione.

[220] «Salvo che il fatto costituisca più grave reato».

[221] La normativa prevede la pena della reclusione da 1 a 6 anni e multa da 5.000 a 15.000 euro.

[222] In AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 18, si legge che la prima condotta di realizzazione consiste nel mettere in atto procedimenti volti alla creazione, lecita o illecita, di materiale pornografico, mentre, la seconda fa riferimento a casi di appropriazione del materiale senza diritto.

[223] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 238.

[224] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 17.

quindi, oltre ad essere già difficile di per sé l'accertamento del dolo specifico, questo potrebbe portare anche ad un esito negativo, creando in questo modo dei vuoti di tutela.

Un punto su cui si è concentrata l'analisi dottrinale è quello riguardante il significato da attribuire al carattere "sessualmente esplicito" che le immagini e i video devono presentare. Il concetto è indeterminato e a differenza di quanto detto per l'art. 600 *ter* c.p. con riguardo al concetto di "materiale pornografico", legislativamente definito nel 2012, il legislatore ha ritenuto di non inserire una definizione puntuale del concetto, rimesso alla valutazione caso per caso del giudice. Non vi è dubbio che il materiale in questione dovrà "attenere al sesso", dovendo le immagini "richiamare la sessualità in modo diretto e inequivoco"[225]: rientreranno quindi nell'espressione quelle immagini o video aventi ad oggetto sia atti sessuali, quale ad esempio il vero e proprio rapporto sessuale, che parti del corpo che siano ricollegabili alla sfera sessuale come il seno, la natica o ancora un corpo interamente nudo. Per quanto riguarda, invece, le immagini dotate di una sessualità "lieve", come ad esempio l'immagine di una donna in intimo, il contesto complessivo dell'immagine sarà oggetto di attenta valutazione[226].

Un altro requisito prescritto espressamente dalla norma è la destinazione delle immagini e dei video, che devono «rimanere privati». Conseguentemente, l'applicabilità della norma sarà esclusa nei casi in cui il materiale sia stato realizzato con lo scopo di essere pubblicato, in qual caso non vi sarebbe una lesione della riservatezza a cui si è rinunciato *ab origine*[227]. In dottrina[228], si è ritenuto che le immagini a sfondo sessuale siano da ritenere "private", a meno che non vi siano degli elementi tali da far presumere che la persona ritratta abbia rinunciato alla riservatezza delle stesse, come ad esempio avendole inserite in una piattaforma.

Dubbi, inoltre, sono emersi nel caso di immagini o video carpiti all'insaputa della vittima. In questi casi, sostenere che la destinazione del materiale venga attribuita da colui che abbia realizzato il materiale sarebbe irragionevole perché la diffusione delle immagini non sarebbe punita in base all'art. 612 *ter* c.p., che prevede un trattamento sanzionatorio più gravoso, ma bensì ai sensi degli artt. 615 *bis* e 617 *septies* c.p.

---

[225] Così come espressamente scritto da AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 20.
[226] CALETTI, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale, cit.,* p. 2069.
[227] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 21.
[228] CALETTI, *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale, op. cit.,* p. 2071.

In materia sono state avanzate due interpretazioni[229]. In base alla prima si ritiene che la natura privata o meno dell'immagine venga attribuita dalla persona ritratta nell'immagine: di conseguenza, l'art. 612 *ter* c.p. richiederebbe l'accertamento di una duplice volontà della persona ritratta, una al momento della manifestazione della sua sessualità riguardo alla possibile diffusione del materiale e l'altra al momento della diffusione stessa. Questa ricostruzione risulterebbe più in linea con la *ratio* della norma, ossia tutela della riservatezza intesa come "libertà di scegliere a chi rivelarsi"[230]. La seconda interpretazione, invece, ricollega la natura privata delle immagini al contesto di realizzazione, circoscrivendo in questo modo l'ambito applicativo della norma a quelle immagini che ritraggono atti sessuali avvenuti nell'ambito di una relazione intima.

È stata ritenuta preferibile la prima interpretazione, che presenta la destinazione e il consenso come "due facce della stessa medaglia"[231]. Quindi, qualora il consenso sia stato dato al momento della realizzazione del materiale, quest'ultimo non si considera più coperto da riservatezza. In caso contrario, la diffusione dovrà essere seguita da espressa autorizzazione[232].

Per quanto riguarda il tema del consenso, questo svolge una funzione negativa di esclusione della configurabilità dell'art. 612 *ter* c.p. Innanzitutto, si deve affermare che il consenso dato a una ripresa a sfondo sessuale o l'invio volontario di immagini intime non si estende automaticamente alla divulgazione delle stesse. La decisione di inviare foto intime o video erotici rientra nella libertà sessuale di colui che è oggetto delle rappresentazioni e la successiva condotta di diffusione di queste in assenza di specifico consenso comporta la configurabilità dell'art. 612 *ter* c.p. Se così non fosse, si rischierebbe di far ricadere la responsabilità della diffusione del materiale sulla stessa vittima della condotta di *revenge porn*[233].

Nei casi, invece, in cui le immagini siano state realizzate all'insaputa della vittima è evidente come il consenso non essendoci stato *ab origine,* non potrà dirsi presente al momento della divulgazione. In queste ipotesi è anche possibile che la condotta costituisca presupposto per l'applicazione non solo dell'art. 612 *ter* c.p., ma anche di altre fattispecie.

---

[229] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 21.
[230] AMORE, *Ivi*., p. 22.
[231] AMORE, *Ivi*., p. 23.
[232] AMORE, *Ibidem.*
[233] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p., op. cit*., p. 1438.

A titolo di esempio, qualora si dovesse ritenere configurabile anche l'art. 615 *bis* c.p., sarà prospettabile un concorso di reati[234].

Ai commi 3 e 4 il legislatore disciplina le ipotesi aggravate.

Il comma 3 stabilisce un aumento di pena qualora la condotta sia «commessa dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva[235] alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici». Trattasi di due aggravanti a effetto comune: la prima si incentra sul rapporto sentimentale che lega la vittima all'autore del reato cogliendo, così, il maggior disvalore offensivo dato dall'abuso dell'affidamento che l'autore pone in essere; la seconda, invece, riguarda gli strumenti telematici o informatici ma data la forte correlazione tra l'emersione del fenomeno del *revenge porn* e la tecnologia, risulta poco ragionevole[236]. Infatti, l'utilizzo di strumenti informatici rappresenta, ad oggi, la modalità base di manifestazione della condotta, comportando quindi una maggior frequenza di contestazioni dell'aggravante piuttosto che dell'ipotesi base.

Al comma 4, invece, sono state inserite due aggravanti a effetto speciale in caso di condotta posta in essere nei confronti di donna in stato di gravidanza o persona in condizione di inferiorità fisica o psichica. Per quanto riguarda la prima, non risulta affatto chiaro se lo stato di gravidanza debba sussistere nel momento in cui i materiali vengono realizzati oppure al momento della diffusione. A rigor di logica sembrerebbe più plausibile la seconda opzione visto l'impatto emotivo che ciò comporterebbe alla donna: tuttavia, il *revenge porn* è una condotta che può venir in essere anche a distanza di tempo rispetto la realizzazione del materiale e ciò aumenterebbe le probabilità di ignoranza dell'autore sullo stato della vittima[237]. A riguardo, vista l'esistenza, *ex* art. 609 *sexies* c.p[238]., di un'"eccezione" relativa all'impossibilità di invocare a propria scusa l'ignoranza, la conseguenza giuridica potrebbe risolversi nell'ammissione dell'autore della condotta di specie a provare l'ignoranza sullo stato di gravidanza[239]. La seconda, invece, sembra essere più ragionevole vista la elevata

---

[234] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p., op. cit*., p. 1439.

[235] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 240, precisa che è stata utilizzata una formula capace di consentire margini di interpretazione ampi e che in realtà è stata rimessa all'autorità giudiziaria l'individuazione di ciò che debba essere inteso come "relazione affettiva".

[236] CALETTI, *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612- ter c.p*, cit., p. 4.

[237] CALETTI, *Ibidem.*

[238] L'articolo stabilisce: «Quando i delitti previsti negli articoli 609 bis, 609 ter, 609 quater, 609 octies e 609 undecies sono commessi in danno di un minore degli anni diciotto, e quando è commesso il delitto di cui all'articolo 609 quinquies, il colpevole non può invocare a propria scusa l'ignoranza dell'età della persona offesa, salvo che si tratti di ignoranza inevitabile».

[239] GRECO, *La pedopornografia telematica e i crimini a sfondo sessuale, op. cit.,* p. 241.

probabilità e facilità con cui soggetti particolarmente vulnerabili possono essere indotti, con falsi propositi, a realizzare materiali intimi senza la reale consapevolezza delle intenzioni del proprio interlocutore[240].

Per quanto riguarda la procedibilità, il comma 5 prevede la possibilità per la persona offesa di presentare la querela nel termine più lungo dei 6 mesi a querela della persona offesa, come nel caso di *stalking* e violenza sessuale, così da consentirle di metabolizzare il danno subito e l'eventuale decisione di affrontare un processo[241]. L'officiosità, invece, è riservata al caso previsto al quarto comma oppure «quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio».

Tirando le fila di quanto emerso in quest'analisi, è evidente come l'introduzione dell'art. 612 *ter* c.p. rappresenti una conquista sociale per il nostro ordinamento ma, al contempo, la convinzione che questo fenomeno possa essere arginato con il solo strumento penale, sia a dir poco azzardata. Infatti, sarebbe opportuno mettere a disposizione strumenti in grado di educare la società circa il fenomeno e prevenire tali condotte disdicevoli, sollecitando una giusta ed efficiente prevenzione[242].

[240] CALETTI, *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612- ter c.p,* p. 4.
[241] AMORE, *La tutela penale della riservatezza sessuale nella società digitale*, *op. cit*., p. 29.
[242] ZANNELLI, "*Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612- ter c.p., op. cit*., p. 1456.

# CONCLUSIONI

Con il presente elaborato si è evidenziato come, dalla nascita di *Internet* ad oggi, la tecnologia si sia evoluta velocemente, arrivando a conquiste inimmaginabili nella mente del legislatore del Codice Rocco. Si pensi alla facilità con cui oggi le persone possono entrare in contattato: anni fa gli incontri erano fisici e con persone già di conoscenza, oggi, invece, nell'arco di pochi secondi è possibile intrattenere una conversazione con più soggetti ignoti. Questa semplicità nel contatto ha non pochi risvolti negativi, soprattutto quando le persone coinvolte sono minorenni, inconsapevoli delle reali intenzioni altrui. Allo stesso modo, la tendenza a rendere lo *smartphone* il proprio portafoglio, rubrica e agenda portatile rende l'individuo un facile bersaglio per coloro che si destreggiano nel cyberspazio.

In questo composito panorama si sono sviluppati i cd. *cybercrimes*, ossia fattispecie criminose che si presentano come nuove modalità di aggressione a beni giuridici già tutelati dall'ordinamento, ma che per le loro caratteristiche mal si conciliano con le norme preesistenti. Infatti, al fine di evitare vuoti di tutela spesso i giudici si sono ritrovati a dover realizzare alcune forzature giuridiche, criticate poi in dottrina.

Alla continua evoluzione tecnologica dovrebbero parallelamente corrisponde lo sviluppo e l'aggiornamento dell'impianto normativo. Nella realtà, si è visto come questa prospettiva spesso non si verifichi.

Tuttavia, a livello internazionale il fenomeno della criminalità informatica è stato al centro dell'attenzione per molto tempo, in particolare dal 1989, con l'intenzione non solo di stimolare gli Stati a favorire una cooperazione, ma anche di stabilire un livello minimo di protezione contro i *cyber crimes*. In questo senso, si sono attivate non solo le istituzioni internazionali, come il Consiglio d'Europa, ma anche organizzazioni internazionali, come l'Organizzazione per la Cooperazione e lo Sviluppo Economico, con il compito di studiare e analizzare il fenomeno.

Il primo passo verso l'adeguamento del nostro diritto penale a quanto stabilito in sede internazionale è stato realizzato nel 1993 con la legge n. 547 sulla criminalità informatica, che, come già sottolineato, non è risultata all'altezza delle aspettative. In particolare, con l'art. 640 *ter* c.p. in tema di frode informatica, il legislatore ha cercato, mediante una formulazione ampia del dettato normativo, di fornire tutela sia al patrimonio che alla segretezza delle comunicazioni e al regolare funzionamento dei sistemi informatici. Tuttavia, la forte indeterminatezza della fattispecie ha dato luogo a diversi dubbi

interpretativi e, a dimostrazione di ciò, in dottrina si sono profilati orientamenti fortemente contrastanti circa i confini applicativi della norma. Forti scontri, ad esempio, hanno riguardato l'inciso "senza diritto" che ancora tutt'oggi rimane una fonte di ambiguità.

Il *deficit* è emerso in modo più evidente nell'analisi del cd. *phishing,* pratica scomponibile in diverse condotte per la quale non è stata ancora introdotta alcuna disposizione *ad hoc*. In questo caso la giurisprudenza ha fatto ricorso a diverse disposizioni già presenti nel Codice, ma senza mai raggiungere un risultato pienamente soddisfacente. L'art. 640 *ter* c.p. è risultato, agli occhi della giurisprudenza di legittimità e parte della dottrina, il giusto candidato da applicarsi ai fini di una corretta tutela, ma la disposizione è stata ritenuta ancora immatura e incompleta per il raggiungimento di questo obbiettivo. La speranza, condivisa dai commentatori, è che la disposizione venga riformulata in termini più precisi, si da essere idonea ricomprendere anche la condotta del *phishing*.

Scopo principale dell'elaborato non è solamente evidenziare come uno strumento all'apparenza così "amichevole" e di ausilio come *internet*, possa facilmente rivelarsi il peggior incubo di molti soggetti, ma anche far emergere le difficoltà con cui il nostro diritto penale si adegua a questi continui e repentini cambiamenti.

In questo senso, oltre all'analisi di quella che è stata la legge protagonista in materia di criminalità informatica, si è approfondito il tema dei reati a sfondo sessuale, dilagati proprio grazie allo sviluppo tecnologico. In particolare, si è parlato di *sexting* e *revenge porn* per il quale il legislatore ha provveduto a inserire una norma apposita nel Codice penale.

Il caso della pornografia domestica, che sfocia poi in una diffusione non consensuale del materiale sia per vendetta, che per goliardia o "pavoneggiamento", per quanto possa essere percepito come una realtà lontana, è un fenomeno insidioso che può portare a conseguenze devastanti per la vittima di queste condotte. A fronte di quanto realizzato in sede internazionale per tutelare la donna rispetto alle diverse forme di abuso sessuale e ai fatti di cronaca di notevole risonanza pubblica, come i casi di Tiziana Cantone e Sarti, anche il nostro legislatore è intervenuto sul punto inserendo il nuovo art. 612 *ter* c.p., nella speranza di porre un freno a queste pratiche.

Nel suo complesso, la nuova disposizione ha creato alcuni contrasti giurisprudenziali in materia di elemento soggettivo e di aggravanti, risultando a tratti "frettolosa" e non del tutto idonea a ricomprendere la pluralità di varianti che possono presentarsi e che vengono tendenzialmente ricondotte nell'ambito del *revenge porn*, come, ad esempio, il *"Vouyerismo digitale".*

Ad avviso di chi scrive, dal presente elaborato si può evincere come la lotta alla criminalità informatica non dovrebbe essere affrontata avvalendosi unicamente dello strumento penale. Il mondo virtuale è intangibile, ma esiste, e può avere impatti importanti sui suoi utenti: la sensibilizzazione ed educazione di questi ultimi alla navigazione consapevole potrebbe rappresentare un aiuto nella prevenzione di questi crimini insidiosi. Infatti, disincentivare gli utenti del *cyber* spazio a inserire informazioni strettamente personali su piattaforme soggette ad *hackering* e invitare le giovani donne che intraprendono relazioni virtuali ad agire con cautela, come anche predisporre misure di sostegno per le vittime di questi reati, può, in aggiunta al diritto penale, permettere di raggiungere un livello di garanzia sufficiente per una società ormai abituata a svilupparsi *online.*

# BIBLIOGRAFIA


AMATO MANGIAMELI A.C.; SARACENI G., *Reati informatici: elementi di teoria generale e principali figure criminose,* Torino, 2015.

AMATO G.; DESTITO V. S; DEZZANI G.; SANTORIELLO C., *I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, Padova, 2010.

AMORE N., *La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.,* in *Leg. pen*., 2020, p. 1 ss.

ANTOLISEI F., *Manuale di diritto penale, Parte speciale*, Milano, 2008.

ARENA M., *La convenzione di Budapest del consiglio d'Europa sulla repressione della criminalità informatica*, Catania, 2021.

BARTOLI R., *La Frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. inform.,* 2011, fasc. 3, p. 383 ss.

BIANCHI M., *Il "sexting minorile" non è più reato?,* in *Dir. pen. cont*., 2016, fasc. 1, p. 138 ss.

BIANCHI M., *I confini della repressione penale della pornografia minorile: la tutela dell'immagine sessuale del minore fra esigenze di protezione e istanze di autonomia,* Torino, 2019.

BLENGINO C., *I reati della rete e la costruzione dei rischi nello spazio digitale,* in *Antigone Quadrimestrale di critica del sistema penale e penitenziario*, 2008, fasc. 3, p. 104 ss.

BORRUSO R.; BUONOMO G.; CORASANTI G.; D'AETTI G., in *Profili penali dell'informatica*, Milano, 1994.

BRENNER S.W., *Cybercrime Metrics: Old Wine, New Bottles*, in *Virginia JL & Tech*, 2004, vol. 9, fasc. 13, p. 1 ss.

BRENNER S.W., *Cybercrime, cyberterrorism and cyberwarfare*, in *Revue internat. droit pénal*, 2006, vol. 77, fasc. 3, p. 453 ss.

CALETTI G.M, *"Revenge porn" e tutela penale. Prime riflessioni sulla criminalizzazione specifica della pornografia non consensuale alla luce delle esperienze angloamericane,* in *Dir. pen. cont*., 2018, fasc. 3, p. 65 ss.

CALETTI G.M., *"Revenge porn". Prime considerazioni in vista dell'introduzione dell'art. 612-ter c.p.: una fattispecie "esemplare", ma davvero efficace?,* in *Dir. pen. cont.,* 2019, p. 1 ss.

CADOPPI A., *L'assenza delle cause di non punibilità mette a rischio le buone intenzioni,* in *Guida. dir*, 2006, fasc. 9, p. 37 ss.

CADOPPI A., *Commentario delle norme contro la violenza sessuale e la pedofilia*, Padova, 2006.

CADOPPI A., CANESTRARI S., MANNA A., PAPA M., *Cybercrime. Diritto e procedura penale dell'informatica,* Torino, 2019.

CAJANI F., *Profili penali del Phishing,* in *Cass. pen*., 2007, fasc. 6, p. 2294 ss.

CALETTI G.M., *Libertà e riservatezza sessuale all'epoca di internet. l'art. 612-ter c.p. e l'incriminazione della pornografia non consensuale,* in *Riv. it. dir. proc. pen*., 2019, fasc. 3, p. 2045 ss.

CARINGELLA F.; DE PALMA M.; FARINI S.; TRINCI A., *Manuale di diritto penale: parte speciale*, Roma, 2017.

CITRON D.; FRANKS M.A, "Criminalizing Revenge Porn", in Wake Forest Law Review, 2014, p. 345 ss.

CONSEIL DE L'EUROPE, *La criminalité informatique: recommandation n° r (89) 9 sur la criminalité en relation avec l'ordinateur et rapport final du comité européen pour les problèmes criminels*, Strasburg, 1990.

CORRADINO M., *La tutela penale del sistema dei pagamenti, in Banca, borsa, tit. cred*., 2001, fasc. 2, p. 121 ss.

COTELLI M., *Pornografia domestica, sexting e revenge porn fra minorenni. Alcune osservazioni dopo la pronuncia delle Sezioni Unite n. 51815/18.,* in *Giur. pen*., 2019, fasc.3, p. 1 ss.

DE NATALE D., *Pornografia minorile e Internet: Brevi note su primi orientamenti dottrinali e giurisprudenziali,* in *Riv. pen*, 2004, fasc. 3, p. 1 ss.

DESTITO V. S.; DEZZANI G.; SANTORIELLO C., *Il diritto penale delle nuove tecnologie,* Milano, 2007.

ELMI T., *La Raccomandazione del Consiglio d'Europa del 9 settembre 1989 n. R (89) - 9 e la Legge 23 dicembre 1993 n. 547 in materia di computer crimes: un'analisi comparativa*, in *Informatica dir*., 1996, fasc.1, p. 116 ss.

FALDUTI M., *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative, in Giur. Pen*, 2017, fasc. 2, p. 1 ss.

FLICK C., *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona,* in *Dir. inform*, 2008, fasc. 4- 5, p. 526 ss.

FLOR R., *Phishing, identity theft e identity abuse.le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen*., 2007, fasc.2-3, p. 899 ss.
FLOR R., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* in *Dir. pen. cont.,* 2010, p. 1 ss.
FONDAROLI D., *La tutela penale dei beni informatici*, in *Dir. Inform*., 1996, fasc. 6, p. 291 ss.
FROSINI V., *Informatica, diritto e società*, Milano, 1992.
FROSINI V., *La criminalità informatica,* in *Dir. inform*., 1997, fasc. 3, p. 489 ss.
FULVI F.R., *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica,* in *Dir. pen. e processo*, 2009, fasc. 5, p. 639 ss.
FUMO M., *La condotta nei reati informatici,* in *Arch. pen.*, 2013, fasc. 3, p. 771 ss.
GALDIERI P., *La criminalità informatica*, in *Riv. elettr. dir. econ. man*., 2013, fasc. 3, p. 19 ss.
GIANNANTONIO E., *I reati informatici*, in *Dir. Inform*., 1992, fasc. 2, p. 335 ss.
GIORDANO V., *L'evoluzione giurisprudenziale del reato di pornografia minorile*, in *Dir. pen. proc, 2019*, fasc. 12, p. 1722 ss.
GRECO G., *I reati informatici in ambito relazionale e a sfondo sessuale: cyberstalking, cyberbullismo e pedopornografia virtuale*, Torino, 2021.
LO MONTE E., *Il c.d. revenge porn nel contesto del 'codice rosso': i limiti della ricostruzione come subspecies della 'violenza di genere'*, in *Iura & Legal system*, 2021, fasc. 1, p. 108 ss.
LUBERTO M., *I reati informatici contro il diritto alla privacy. La tutela fornita dal d. lg n. 196 del 2003 e dal Codice penale*, in *Giur. Mer*., fasc. 3, 2008, p. 1 ss.
MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica,* in Crit. dir., 1994, fasc. 4, p. 12 ss.
MANNA A.; RESTA F., *I delitti in tema di pedopornografia, alla luce della legge 38/2006. Una tutela virtuale?* in *Dir. Int.*, 2006, fasc. 3, p. 221 ss.
MARCELLI G., *I reati informatici a danno dell'istituto nazionale della previdenza sociale (I.N.P. S)*, in *Dir. inform*, 1993, fasc. 4-5, p. 1007 ss.
MASI A., *Frodi informatiche e attività bancarie*, in *Riv. pen. econ*, 1995, fasc. 7, p. 427 ss.
MATTARELLA A., *Il cybercrime nell'ordinamento italiano e le nuove prospettive dell'Unione Europea e delle Nazioni Unite*, in *Dir. pen. proc.,* 2022, fasc. 6, p. 809 ss.
MATTARELLA A., *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informatica,* in *Arch. pen.,* 2022, fasc. 3, p. 41 ss.

MAZZA F., *Prevenzione e repressione in tema di reati informatici*, in *Oss. pen*., 2014, p. 1 ss.

MILITELLO V., *"Nuove esigenze di tutela penale e trattamento elettronico delle informazioni"*, in *Riv. trim. pen. econ*., 1992, p. 365 ss.

MUCCIARELLI F., *Commento all'art. 10 della l. 23/12/1993. n. 547*, in *Leg. pen*., 1996, p. 136 ss.

PALOMBI E.; PICA G., *Diritto penale dell'economia e dell'impresa*, Torino, 1996.

PARODI C.; SELLAROLI V., *Diritto penale dell'informatica: reati della rete e sulla rete,* Milano, 2020.

PARKER D.B., *Computer related crime*, in *Journal of Forensic sciences*, 1974, p. 292 ss.

PETRINI D., *La tutela del buon costume,* in *Dir. inform*., 2011, fasc. 3, p. 445 ss.

PECCIOLI A., *Un ulteriore intervento a tutela dei minori (I parte),* in *Dir. pen. proc*, 2013, fasc. 3, p. 137 ss.

PECCIOLI A., *La rilevanza penale della pedopornografia ad uso personale tra punti fermi e residui profili critici,* in *Dir. pen. proc*., 2022, fasc. 9, p. 1195 ss.

PECORELLA C., *L'abuso dei distributori automatici di banconote,* in *Riv. it. dir. e proc. pen.,* 1990, fasc. 2, p. 198 ss.

PECORELLA C., *Il nuovo diritto penale delle carte di pagamento*, in *Riv. it. dir. proc. pen*., 1993, fasc.1, p. 235 ss.

PECORELLA C., *Diritto penale dell'informatica,* Padova, 2006.

PELLEGRINI D., *Uso non autorizzato del computer. Limiti e prospettive della tutela penale*, in *Dir. inform*, 1987, p. 289 ss.

PICA G., *Diritto penale delle tecnologie informatiche: computer's crimes e reati telematici internet banche dati e privacy,* Torino, 1999.

PICOTTI L., *Il diritto penale dell'informatica nell'epoca di internet,* Padova, 2005.

PICOTTI L., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale,* in *Dir. internet*, 2005, fasc. 2, p. 189 ss.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa LEGGE 18 MARZO 2008, N. 48,* in *Dir. pen. e processo,* 2008, fasc. 6, p. 696 ss.

PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo,* in *Dir. internet*, 2008, fasc. 5, p. 437 ss.

PICOTTI L., *I profili di diritto sostanziale, in La ratifica della Convenzione Cybercrime del Consiglio d'Europa,* in *Dir. pen. proc*., 2008, fasc. 6, p. 700 ss.

PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec*., 2011, fasc. 4, p. 827 ss.
PICOTTI L., *I primi vent'anni della Convenzione di Budapest nell'ottica sostanzialista e la mancata ratifica ed esecuzione del Primo Protocollo addizionale contro il razzismo e la xenofobia*, in *Dir. pen. proc*, 2022, fasc. 8, p. 1030 ss.
PIETRELLA T., *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle Botnets*, in *disCrimen,* 2021, p. 1 ss.
PITTARO P., *Le norme contro la pedofilia- A) Le norme di diritto penale sostanziale,* in *Dir. pen. proc*, 1998, fasc. 10, p. 1225 ss.
RECCIA E., *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria,* in *Arch. pen.,* 2022, p. 1 ss.
RESTA S., *lnformatica, telematica e computer crimes,* in *Infor. dir.,* 1997, fasc. 1, p. 143 ss.
RESTA S., *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura,* in *Corriere del Merito*, Torino, 2008.
ROMANO B., *Delitti contro la sfera sessuale della persona*, Padova, 2017.
ROMANO B., *La pornografia minorile nella (nuova) lettura delle Sezioni Unite: dal pericolo concreto al reato di danno,* in *Cass. pen*., 2019, fasc. 2, p. 587 ss.
SARZANA DI SANT' IPPOLITO C., *Criminalità e tecnologia: il caso dei computer-crimes,* in *Rass. penit. crim*, 1979, fasc. 1- 2, p. 53 ss.
SARZANA DI SANT'IPPOLITO C., *Sicurezza informatica e lotta alla cibercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislative,* in *Dir. Internet*, 2005, fasc.5, p. 437 ss.
SARZANA DI SANT' IPPOLITO C., *Informatica, internet e diritto penale,* Milano, 2010.
SCARCELLA A., *Tassatività e determinatezza della nozione di «pornografia»: la Cassazione apre al diritto comunitario,* in *Dir. pen. proc*, 2010, fasc. 8, p. 973 ss.
SCOPINARO L., *Internet e i reati contro il patrimonio,* Torino, 2007.
SIEBER U., *La tutela penale dell'informazione,* in *Riv. trim. pen. econ*., 1992, p. 492 ss.
TIEDEMANN, *Phénoménologie des infractions économiques*, in *Aspects criminologiques de la délinquance d'affaires*, Strasburg, 1978, p. 231 ss.
VERRI A., *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE. Approvate dal legislatore europeo nuove norme contro l'abuso, lo sfruttamento sessuale dei minori e la pornografia minorile,* in *Dir. pen. cont.,* 2010, p. 1 ss.
VITALE F., *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime,* in *Arch. pen.*, 2015, fasc. 1, p. 1 ss.

VIZZARDI M., *Sull'"adescamento" di minore tramite social network e il tentativo di atti sessuali con minorenne,* in *Dir. pen. cont*., 2012, fasc. 1., p. 196 ss.
ZANNELLI C., *"Revenge porn". Pregi e aporie della nuova fattispecie di cui all'art. 612-ter c.p.,* in *Dir. fam.*, 2021, fasc. 3, p. 1429 ss.