QUESITI

PIER PAOLO CASALE

Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento"[1]

L'articolo si propone di esaminare il reato di accesso abusivo a sistema informatico o telematico alla luce dell'evoluzione tecnologica, laddove le nuove azioni criminose appaiono di non facile inquadramento nel delitto *ex* art. 615-*ter* c.p., a fronte, anche, di una difficile intesa in merito al bene giuridico che la norma intende tutelare. In particolare, l'A. ha concentrato la propria attenzione sulla pratica della c.d. "divulgazione responsabile" oggetto di una recente pronuncia, cercando di comprendere se - e come - questa condotta, ormai generalmente riconosciuta e realizzata dagli operatori informatici e dagli *hacker*, possa, sotto un profilo dogmatico, influire sulla rilevanza penale del fatto commesso.

First "law" of IT security: "A secure computer is a computer that is turned off

The article aims to examine the crime of unauthorized access to a computer or telematic system in the light of technological evolution, where the new criminal actions appear to be difficult to classify in the crime pursuant to art. 615-ter of the Criminal Code even in the face of a difficult consensus on the substance legal right that the rule is intended to protect. In particular, the A. He has focused attention on the practice of so-called "Responsible disclosure", the subject of a recent ruling, trying to understand if and how this conduct, despite the widely accepted and implemented by IT professionals and hackers, can, from a dogmatic point of view, affect the criminal relevance of the crime committed.

1. *Considerazioni introduttive*. Sono trascorsi quasi trent'anni dall'introduzione, nel nostro ordinamento, del delitto di Accesso abusivo a sistema informatico o telematico, attraverso la legge n. 593 del 1993, con la quale il legislatore, nell'intento di corrispondere alle richieste di punizione provenienti dalle fonti sovranazionali[2], si è occupato in modo organico di san-

[1] Questa "legge" – con pari valore di quelle declinate da ASIMOV, *Io, robot*, (trad. it. SERRA), Milano, 2004, per la robotica – è stata individuata da Eugene H. Spafford, il quale ha affermato nella sua versione completa: «*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts*».

[2] Si era tentato attraverso interpretazioni analogiche (mascherate come estensive) di sanzionare azioni peculiari che vedevano l'utilizzo degli strumenti tecnologici allora esistenti. Si veda, a titolo di esempio, per il delitto in parola, la fattispecie della violazione di domicilio *ex* art. 614 c.p. (cfr. TAVASSI LA GRECA, *L'approccio normativo alla criminalità informatica*, in *Adir*, 2003, 3 reperibile all'indirizzo *www.adir.unifi.it*). Nel 1983 l'Ocse iniziò ad occuparsi del fenomeno criminoso tanto da pubblicare nel 1986 un *dossier* sul punto (*Computer Related Crime: Analysis of Legal Policy*) con il quale proponeva accorgimenti e particolari discipline volte a fronteggiare le nuove condotte antidoverose. Nel 1989 il Consiglio d'Europa adottò la raccomandazione sulla criminalità informatica [R (9)] con la quale approntò la prima distinzione tra i reati di "vecchia concezione" e i reati informatici "c.d. propri", introducendo una sotto distinzione nella quale individuava quelli che indispensabilmente sarebbe stato necessario promulgare in tutti gli ordinamenti appartenenti alla compagine europea e quelli che

zionare tutte quelle azioni che danneggiavano interessi meritevoli di tutela in questo peculiare settore.
A fronte della successiva ulteriore evoluzione tecnologica e dell'accelerazione che la stessa ha avuto in questo nuovo millennio, appare dunque opportuno tracciare lo "stato dell'arte" e comprendere se il delitto di cui all'art. 615-*ter* c.p. possa ritenersi ancora funzionale a fronteggiare tutte quelle condotte, lesive della sicurezza informatica, le quali vengono comunemente perpetrate nella virtualità delle nostre "esistenze digitali". In particolare, l'oggetto della presente indagine si soffermerà sull'analisi del primo comma della disposizione in parola e, in particolare, sull'elemento oggettivo descritto con l'espressione «abusivamente si introduce nel sistema informatico o telematico protetto da misure di sicurezza»; a ben vedere, già al tempo della sua introduzione nel Codice penale, esso rappresentava la chiave di volta del fatto tipico

potevano ritenersi opzionali (cfr. FLOR, '*Cyber-criminality': Le fonti internazionali ed europee*, in *Cybercrime*, Milano, 2019, 99 s.).

penalmente rilevante[3] e destò le maggiori perplessità della dottrina sotto il profilo tecnico-normativo[4].

2. *Alcune premesse di natura criminologica*. Ancor prima di addentrarsi nell'analisi poc'anzi menzionata, appare utile comprendere quale sia il fenomeno sociale che ha dato vita al mondo dell'attacco informatico, procedendo a una valutazione della natura e della distinzione tra le figure che qualificano il soggetto agente chiamato convenzionalmente *hacker*. Nella tradizione anglo-americana, con il termine *hacker* si è inteso qualificare la persona dotata di particolari competenze e capace di intaccare un determinato sistema *hardware* o *software*[5]; gli *hacker* hanno raggiunto la fama nella cultura di massa per

[3] Invero, il secondo periodo del primo comma dell'art. 615 *ter* c.p. si occupa di sanzionare i comportamenti posti in essere da soggetti provvisti di appositi permessi (o credenziali) nell'utilizzo di sistemi informatici o telematici si intrattengano – o utilizzino gli stessi – per esigenze ultronee rispetto a quelle per cui detenevano tali autorizzazioni di accesso. La giurisprudenza di legittimità si è soffermata nell'esaminare il caso in cui l'agente fosse un pubblico ufficiale o incaricato di pubblico servizio. La sentenza di riferimento è Cass., Sez. un., 18 maggio 2017, in *Riv. Ita. Dir. Proc. Pen.*, 2018, 4, 2256 ss. nella quale, in prima battuta si è inteso ribadire quanto già era stato affermato con la sentenza Casani, ossia il reato in questione si sarebbe configurato allorquando un soggetto, pur avendo i permessi (e cioè le *password* di accesso a un sistema) sarebbe entrato in esso per scopi o finalità eccentriche rispetto a quelle per cui gli era stata concessa l'autorizzazione. L'elemento di novità è da ravvisarsi nella valutazione ulteriore compiuta dal giudice di legittimità, concernente la peculiarità dell'agente (*status* di p.u. o incaricato di p.s.) non soggetto a particolari restrizioni nei suoi poteri di accesso nel sistema pubblico, laddove in ossequio agli artt. 54, 97 e 98 Cost. è tenuto a seguire una particolare "etica pubblica", la cui violazione comporta l'eccesso di potere. Pertanto, se egli accede o si mantiene nel sistema informatico, pur utilizzando le proprie credenziali legittimante concesse «per ragioni ontologicamente estranee o comunque diverse rispetto a quelle per le quali, soltanto, la facoltà gli è attribuita» commette il reato di cui all'art. 615 *ter* c.p. (*ex multis*, SARACENI, *I reati informatici. Dalla diffusione di 'virus' all'accesso abusivo*, in AMATO MANGIAMELI-SARACENI, *I Reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, 2019, 68 s.; MENDICINO, *La condotta del pubblico ufficiale, come dell'investigatore privato, che mira al raggiungimento di un fine non istituzionale integra reato*, in *Dir. giust.*, fasc. 140, 2017, 8; FLOR, *La condotta del pubblico ufficiale fra violazione della 'voluntas domini', "abuso" dei profili autorizzativi e "sviamento di poteri"*, in *Dir. pen. proc.*, 2018, n. 4, 506 ss.; FLOR, *Verso una rivalutazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. cont.*, 2011, 126 ss.; SALVADORI, *Quando un 'insider' accede abusivamente ad un sistema informatico o telematico. Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. economia,* 2012, 369 ss.; PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004).

[4] Cfr. BERGHELLA-BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, fasc. 9, 1995, 2329 ss.; GIANNANTONIO, *L'oggetto giuridico dei reati informatici*, in *Cass. pen.*, fasc. 7-8, 2001, 2029 ss.; SPAGNOLETTI, *Art. 615 'ter' c.p.: il domicilio informatico tra profili dogmatici e problemi applicativi*, in *Giur. merito*, fasc. 1, 2004, 181 ss.

[5] Il c.d. *hacking* e la sua filosofia di vita partì dall'edificio 26 del MIT (*Massachusetts Institute of Technology*), precisamente nel 1958 presso il *Tech Model Railroad Club*, da appassionati di modellismo ferroviario. Il gruppo di amici si occupava di controllare una particolare modellino di

mezzo della filmografia[6] e sono diventati un fenomeno pop con l'avvento del *world-wild-web*, che li ha trasformati in vere e proprie icone da emulare.
Tra gli addetti ai lavori della sicurezza informatica si è giunti ad un'apposita classificazione di tali individui che si destreggiano abilmente nella rete; in particolare, i *cyber*-criminali vengono genericamente chiamati "*hat*" e si usa distinguerli in tre macrocategorie:
i) i primi, c.d. *black*, sono *hacker* o, per meglio dire, *cracker*, che eseguono attacchi per un proprio tornaconto strettamente personale;
ii) i secondi sono chiamati white, anche noti come *ethical hacker*, e sono figure specializzate nel compiere attacchi, perché ingaggiati con contratto dai proprietari del sistema informatico; essi, in buona sostanza, eseguono incursioni "benigne" al solo scopo di verificare se la sicurezza del *software* del contraente sia idonea a fronteggiare eventuali tentativi di intrusione;
iii) da ultimo, i *grey*, ovvero figure intermedie, le quali agiscono secondo i casi sia come *white hat* sia come *black hat*, con l'unica discriminante legata alla propria insindacabile decisione e valutazione nel caso concreto.
In realtà, tale suddivisione risulta alquanto problematica poiché i contorni delle tre categorie che la compongono, se in via astratta appaiono ben netti, nella realtà dei casi sono alquanto sfumati; ad ogni modo, la citata tripartizione è assai utile al fine di meglio comprendere i motivi a delinquere che animano il loro agire e, nel prosieguo, saranno utili nell'intendere l'azione di c.d. R.V.D. (*Responsible Vulnerability Disclosure*) che verrà infra descritta; infatti, i principali scopi che muovono i cyber-criminali appaiono essere, in ordine di importanza: il profitto economico, la dimostrazione delle proprie capacità, le prove di forza con altri concorrenti nella comunità internauta e, da ultimo, la protezione della sicurezza dei dati dei cittadini.

3. *L'accesso abusivo a un sistema informatico: il fatto tipico*. L'accesso abusivo a un sistema informatico o telematico può consumarsi attraverso violazioni

---

ferrovia particolarmente complesso che diede vita a due distinti correnti: la prima, chiamata *"knife-and-paintbrush"* letteralmente "coltello e pennello", che impiegava il proprio tempo a riprodurre modelli di vagoni ferroviari da anni fuori produzione oppure alla ricostruzione di paesaggi o edifici; la seconda, soprannominata *"Signal-and-Power"* ovvero "segnali e corrente", questo gruppo era invece interessato al complessivo *layout,* occupandosi prevalente dello studio delle tecnologie per la costruzione della rete elettrica che governava gli scambi dei trenini, che chiamavano *"the system",* per una storiografia completa sulla figura del pirata informatico cfr. LEVY, *Hackers. Gli eroi della rivoluzione informatica*, (*trad. it.* GUARNERI-PIERCECCHI), Milano, 2002.

[6] Nella cultura *cyberpunk* i principali film che hanno avuto ad oggetto gli *hacker* sono *Wargames* (1983), *Hackers* (1995), Jhonny Mnemonic (1995), *Matrix* (1999), *Citizenfour* (2015).

da qualificarsi come "domestiche"[7], oppure per mezzo di particolari operazioni che richiedono una profonda conoscenza dei linguaggi di programmazione e della rete *internet*.
La disposizione incriminatrice attribuisce un ruolo essenziale, ai fini della rilevanza penale, alla violazione delle misure di sicurezza[8] approntate per difendere il sistema, laddove non è da considerarsi come punibile la mera azione consumata priva di autorizzazioni, bensì solo quella che trasgredisca i limiti imposti dalle protezioni adottate dal titolare del sistema.
Ciò premesso, al fine di meglio comprendere le caratteristiche materiali della "introduzione" penalmente rilevante, è necessario anzitutto comprendere le prerogative che la misura stessa presenta all'interno del c.d. "mondo virtuale".
La protezione di un sistema può essere rappresentata come una "porta fisica" che permette l'accesso ad una stanza; questo ingresso può assumere diverse configurazioni, intimamente connesse ai vari tipi di incursione che un soggetto può materialmente compiere:
i) la porta, per usare una metafora, può essere aperta, nel senso che chiunque tenti di accedere non troverà alcun ostacolo all'ingresso né alcuna richiesta di identificazione;
ii) oppure la porta può essere "chiusa a chiave": in questo secondo caso, solo il soggetto in possesso delle chiavi di autorizzazione potrà legittimamente accedervi;
iii) tuttavia, ci possono essere casi in cui la porta è sì chiusa, ma non "a chiave", nel senso che "girando la maniglia" chiunque potrà accedervi senza trovare resistenza;
iv) da ultimo, all'interno di un sistema informatico si può dare una situazione parificabile ad una "porta socchiusa", nel senso che l'ingresso appare a un

[7] Con l'espressione accesso abusivo a sistema informatico "domestico", si vuole intendere tutte quelle condotte che non presentano particolari caratteristiche sotto il profilo tecnico operativo e che possono essere realizzate da qualsiasi utente dello spazio *web*. Recentemente la Cassazione si è occupata di un peculiare caso (cfr. Cass., Sez. V, 31 gennaio 2019, in *Quot. giur. web*) in cui dove l'imputato era entrato abusivamente sia nel profilo *facebook* della vittima (a cui era legato sentimentalmente) sia nell'*account* di posta elettronica con le sue credenziali. Non pago, procedeva anche a modificare le relative *password* e prendeva contatto con l'*ex* fidanzato, con il preciso intento di arrecare danno alla persona offesa. In altro procedimento la Corte di legittimità (cfr. Cass., Sez. V, 22 gennaio 2019, in *Quot. giur. web*) ha confermato che il reato *ex* art. 615 *ter* c.p. si configura tra coniugi anche quando il marito conosca le chiavi di accesso perché, fornitegli in passato dalla moglie (per un primo commento alle sentenze in parola cfr. BASSOLI, *L'accesso abusivo a sistema informatico e la violazione del domicilio digitale*, in *Sicurezza Giust. Web*, I/MMXIX, 28).
[8] La parte informatica è stata redatta grazie alla consulenza del Dott. Marco DAL BROI, *DPO e Penetration Tester*.

primo sguardo delimitato, ma in realtà la "porta" risulta in sé aperta per chiunque osservi bene la soglia.
Come ben si può comprendere da queste metafore, vi sono numerose e differenti possibilità per accedere a un sistema informatico.
Quanto all'ipotesi sub i), la stessa appare tendenzialmente priva di rilevanza penale, in quanto sprovvista del requisito legale *ex* art. 615-*ter* c.p. delle "misure di sicurezza" in ipotesi violate dal soggetto agente.
L'ipotesi sub ii), invece, rappresenta il caso c.d. "da manuale", trattandosi del classico attacco informatico realizzato dal *black hat* violando le misure sicurezza apposte dal titolare o dall'utilizzatore del sistema informatico; ritornando alla similitudine proposta, in questi casi il soggetto agente troverà una porta chiusa a chiave e otterrà l'accesso manomettendo la serratura, i cardini o il materiale con cui la porta stessa è costruita: questo sarà il tipico accesso abusivo al sistema informatico sanzionato penalmente dall'art. 615-*ter* c.p.
Dubbi interpretativi possono, invece, sorgere allorquando ci si trovi al cospetto del c.d. "attacco SQL injection", il quale può astrattamente essere sussunto nelle ipotesi sopra indicate sub iii) o iv), secondo i casi: in questa ipotesi, il database è tecnicamente nascosto o, per meglio dire, non consultabile da un visitatore privo di particolari competenze, ma in realtà è accessibile a chiunque interroghi correttamente il server, ottenendo così le informazioni in esso contenute. Secondo la giurisprudenza, il delitto in parola avrebbe il preciso scopo di proteggere quello che è stato definito "domicilio informatico": esso, secondo tale logica, costituirebbe un luogo assimilabile a una abitazione o una privata dimora, ove l'individuo estrinseca la propria proiezione spaziale ed esercita il proprio diritto allo *ius escludendi alios*. Alla luce di questo tipo di lettura, la tecnica di "pirateria informatica" menzionata si sottrarrebbe alla previsione del reato *de quo*, poiché, nei casi appena menzionati, non pare verificarsi una vera e propria incursione all'interno del sistema e, di conseguenza, non verrebbe leso né il luogo né lo spazio informatico; infatti, da un lato, non è stata violata alcuna misura di sicurezza formalmente intesa; dall'altro, non è stato compiuto alcun accesso al server[9].
Al fine di comprendere se anche queste ultime ipotesi rientrino o meno nel paradigma dell'art. 615-*ter* c.p., appare opportuno analizzare il bene giuridico

[9] Parte della dottrina, tuttavia, afferma che l'"accesso" si verificherebbe quando l'internauta si pone in relazione con il diverso sistema informatico, il quale compie precise operazioni a fronte di comandi lanciati dal navigante, costringendo il calcolatore ad eseguirle ottenendo così le informazioni in esso contenute (cfr. sul punto SALVADORI, *L'esperienza giuridica degli Stati Uniti D'America in materia di hacking e cracking*, in *Riv. It. dir. proc. pen.*, Vol. 51, fasc. 3, 2008, 1343 ss.).

tutelato da tale fattispecie incriminatrice, alla luce cioè del fondamentale principio di offensività[10].

La dottrina[11], sul punto, dibatte da tempo in merito a quale bene giuridico la norma sia chiamata a proteggere, cercando di superare l'interpretazione c.d. "originalista"[12] seguita dal giudice di legittimità[13].

Infatti, l'idea di ancorare in via analogica il bene giuridico della fattispecie in parola a quello tutelato dall'art. 614 c.p. appare ormai superata rispetto a un mondo tecnologico in perenne evoluzione.

Le tesi più aggiornate, trovando sponda nelle fonti giuridiche sovranazionali[14], hanno ritenuto di individuare due distinti interessi meritevoli di tutela, capaci di evitare che potenziali nuove modalità di introduzione abusiva possano rimanere escluse dalla coperta della sanzione penale[15]: la prima è rappresentata

---

[10] «L'offensività senza il bene giuridico è inconcepibile già lessicalmente. Infatti, si può trattare dell'offensività senza fare dogmatica in termini di categorie del reato, ma solo di principi, ma per una elaborazione scientificamente completa solo l'analisi degli elementi strutturali del reato consente di rispondere alle obiezioni che continuamente vengono sollevate – in chiave descrittiva o prescrittiva, poco importa – contro il bene giuridico e, nello stesso tempo, contro l'offensività che lo presuppone, o al limite contro la loro capacità selettiva. La dogmatica di principi presuppone una dogmatica di categorie, ma non la sostituisce, e anzi la implementa, rivitalizzandola. Senza il bene giuridico, infatti, il discorso sull'offesa non ha una base strutturale» così DONINI, *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Dir. pen. cont.*, fasc. 4, 2013, 8.

[11] Alcuni autori sostengono che il reato introdotto nel 1993 sia plurioffensivo, poiché l'azione è capace di ledere una diversità di beni giuridici eterogeni (vd. SARACENI, *I reati informatici*, cit., 60 e nt. 5) tra cui il diritto alla riservatezza, diritti di natura patrimoniale fino a toccare interessi collettivi (sul punto CUOMO-RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009, 94 s.).

[12] «La normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio, perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono l'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale». Così la relazione al Disegno di legge in materia di "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità organizzata*", 11 giugno 1993.

[13] Cfr. Cass., Sez. II, 20 maggio 2019, in BORGOBELLO, *La Cassazione sul rapporto tra accesso abusivo a sistema informatico, frode informatica e detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, in *Giur. pen.*, 2020, 1; Cass., Sez. V, 26 ottobre 2012, in *www.dirittoegiustizia.it*; Cass., Sez. VI, 27 ottobre 2004, inedita.

[14] Ci si riferisce alla Convenzione sulla Criminalità Informatica (*Convention on Cybercrime*) del 23.11.2001, che ha visto la ratifica da parte dell'Italia con la l. n. 48/2008 e a quanto previsto dagli articoli 10 della Cedu e all'art. 11 della Carta di Nizza (per un approfondimento sul contenuto della Convenzione cd. di Budapest si veda FLOR, '*Cyber-criminality': le fonti internazionali ed europee*, in *Cybercrime*, Torino, 2019, 101 ss.).

[15] Si è utilizzato - per convenzione generalmente riconosciuta - parificare lo spazio virtuale a quello di un ambito abitativo che abbia porte in cui poter accedere e dove al suo interno possano essere conservati dati di diversa natura. Nulla vieta, invece, di considerare tale ambito in diverso modo: si pensi ad esempio ad un cassetto nel cui interno sia possibile conservare cose; ciò semplicemente smonterebbe l'idea stessa di domicilio svuotandone di contenuto (conforme sul punto TAVASSI LA GRECA, *L'approccio normativo*, cit., 12 ss.).

dalla "riservatezza informatica" rispetto ai diritti della persona e consisterebbe «nell'assicurare a ciascuno l'utilizzo o godimento indisturbato ed esclusivo degli [spazi] anche solo virtuali che possono permettere un pieno sviluppo ed una libera estrinsecazione della persona umana»[16]; la seconda, costituita dalla "sicurezza informatica" qualificata come interesse super-individuale, è volta ad assicurare che i dati rimangano perfetti nella propria integrità e siano fruibili dalla comunità sotto ogni forma[17].

Fra le condotte che possono mettere a rischio entrambi i citati interessi vi è il c.d. "attacco di DDos", letteralmente *Distribuited Denial of Service*, che si realizza procurando l'interruzione di un servizio informatico mediante l'interrogazione di un server da parte di un numero eccessivo di connessioni, causandone il c.d. *down*. Un esempio pratico è stata l'incursione subìta dal servizio di gestione *e-mail* con base in Svizzera chiamato Protonmail: nel caso di specie, il sito *internet* (e il relativo *server* su cui è possibile andare a visitare gli account di posta elettronica) non è stato più accessibile dal 3 novembre 2015 al 10 novembre 2015, a causa di un attacco congiunto da parte di due gruppi distinti di *hacker* con differenti capacità tecniche, ma aventi un medesimo intento: procurare più danni possibili, negare l'utilizzo del server di posta agli utenti ed estorcere denaro dalla società colpita.

Tuttavia, i beni giuridici sopra tratteggiati, e in particolar modo il primo – vale a dire quello della "riservatezza informatica" – appaiono eccessivamente indeterminati e sfuggenti, tanto che, ove adottati quale parametro interpretativo della fattispecie incriminatrice, affiderebbero al giudice penale[18] quasi un potere di "integrare", in sede ermeneutica, la fattispecie medesima, in violazione dei principi di legalità e di "prevedibilità"[19].

---

[16] SALVADORI, *I reati contro la riservatezza informatica*, cit., 662 e 665. Tuttavia, a modesto avviso dello scrivente, la categoria di "riservatezza informatica" parrebbe non avere caratteri propriamente distintivi rispetto al concetto di *privacy* e di tutela dei dati personali, se pur mantiene il pregio di proteggere spazi e servizi di cui ogni "navigatore moderno" fruisce nella rete *web*.

[17] Per un'analisti comparativa tra bene giuridico personalistico e bene giuridico super-individuale cfr. COCCO, *Beni giuridici funzionali 'versus' Ben giuridico personalistico*, in *Studi in onore di Giorgio Marinucci*, a cura di Dolcini, Paliero, Milano, 2006, 179 ss.

[18] Per approfondire la discrezionalità come interpretazione della fattispecie astratta CARUSO, *La discrezionalità penale. Tra «tipicità classificatoria» e «tipologia ordinale»*, Padova, 2009, 22 ss.

[19] Sul concetto di prevedibilità della norma penale ADDANTE, *Il principio di prevedibilità al tempo della precarietà*, in *questa Rivista* 2, 2019, 9 ss.; CASTRONUOVO, *Clausole generali e prevedibilità delle norme penali*, in *Quest. giust.*, 3, 45 ss.; VIGANÒ, *Il principio di prevedibilità della decisione giudiziale in materia penale*, in *www.penalecontemporaneo.it*, 1 e in particolare 8 ss.

Ulteriore condotta che solleva dubbi in merito alla struttura del reato è l'attacco c.d. "exploit di vulnerabilità": questa modalità è tendenzialmente utilizzata nei confronti di sistemi operativi o di *software* non aggiornati e si basa sullo sfruttamento delle criticità non risolte per mancato ammodernamento del programma o dalle scoperte di c.d. Zero Day[20].

La questione può essere proposta in questi termini: il mancato aggiornamento del *software*, inteso come suo omesso adeguamento allo stato della tecnica, può far ritenere insussistente l'elemento costitutivo richiesto dalla fattispecie di accesso abusivo? La dottrina sostiene che, affinché la condotta materiale assuma rilevanza penale, è sufficiente che il sistema in cui ci si introduce, senza essere autorizzati, sia dotato di una qualsivoglia forma di protezione, a prescindere dal livello di complessità o grado di efficacia; inoltre, non rileverebbe il fatto che l'elemento di sicurezza sia costituito da una banale *password* di *default*, come quella di base che viene inserita da ogni casa produttrice al momento del rilascio di un programma e non sia stata mai modificata dall'acquirente[21].

Tuttavia, il caso di "attacco exploit" risulta parificabile, per usare una metafora, alla situazione in cui un portone di legno sia sì "chiuso a chiave", ma la serratura non sia in alcun modo aggiornata rispetto al progresso tecnologico, tanto che il pirata informatico, anche solo adoperando una forcina per capelli, sarebbe in grado di aprirlo. In alternativa, l'*hacker* potrebbe utilizzare la fragilità in un altro modo ovvero bypassando la misura di sicurezza per accedere al sistema: in tale caso, si potrebbe parlare di vulnerabilità c.d. "esposta all'esterno"[22], che ricorre quando – in senso figurato – ci si trovi in presenza di una finestra di dimensioni pari all'uscio, lasciata aperta e collocata accanto alla porta chiusa tanto da rendere inesistente la misura di sicurezza.

In una analoga fattispecie, ad esempio, il Tribunale dell'Aquila[23] ha ritenuto di dare una differente risposta a quanto interpretato dalla dottrina, sostenen-

---

[20] Con l'espressione *Zero Day* ci si riferisce alla vulnerabilità ancora ignota ai creatori del *software* e di cui il pirata informatico approfitta per compiere l'*exploit*.

[21] Così SALVADORI, *I reati contro la riservatezza informatica*, cit., 677 s.; di parere conforme CUOMO-RAZZANTE, *La nuova disciplina*, cit., 101 e, come riferito da SARACENI, *I reati informatici*, cit., 63 nt. 11, lo stesso ZICCARDI afferma «l'esistenza del mezzo di protezione (anche se, in concreto, scarsamente efficace) ha la semplice funzione di rendere esplicito e inequivoco che si è in presenza di un divieto di accesso al sistema informatico» (ZICCARDI, *Manuale breve di informatica giuridica*, Milano, 2008, 262).

[22] Secondo il *Common Vulnerabilities and Exposures* (CVE), con il termine "esposizione", in via di massima, è da intendersi un errore nel software/nella sua configurazione che permette l'accesso a funzioni ed informazioni.

[23] Trib. Aquila, 13 marzo n. 2010 sent. n. 144 (dep. 20 marzo 2010) in *bdprof.ilsole24ore.com*, affoliazione 5 della pronuncia (citata da SARACENI, *I reati informatici*, cit., 64 nt. 12).

do che il sistema informatico deve essere in genere preservato dall'amministratore: nella *ratio legis*, secondo il giudice monocratico, le misure di sicurezza sono «destinate a svolgere un'importante funzione di responsabilizzazione della vittima, nel senso che costui potrà confidare nella repressione penale solo se in precedenza avrà protetto il sistema informatico/telematico secondo le tecniche elaborate dalla vigente tecnologia».
A nostro sommesso avviso, per "tecniche elaborate" dovrebbe intendersi anche l'utilizzo di c.d. *patch* di correzione di vulnerabilità, il cui mancato impiego porterebbe all'esclusione della consumazione del reato di accesso abusivo.

4. *Una fenomenologia peculiare: la c.d. divulgazione responsabile* (responsible disclosure). Gli aspetti inerenti alla vulnerabilità di un sistema informatico o telematico richiedono un ulteriore approfondimento, a fronte di una prassi ormai in voga, consistente nella procedura di c.d. "divulgazione responsabile" (*responsible disclosure*).
La *responsible disclosure* si sostanzia nel comportamento da parte di un *white hat* il quale, avendo scoperto (causalmente o scientemente) la vulnerabilità di un sito internet, di un *software* o di una applicazione informatica, si prodiga anzitutto di avvisare il produttore o il fornitore del servizio, affinché provveda a emendare e correggere il sistema informatico. Qualora, entro un certo termine, egli non trovi riscontro alla segnalazione, lo scopritore si ritiene allora, nella prassi, legittimato a divulgare l'errore tecnico individuato, utilizzando i *social network*; molto spesso, ciò avviene pubblicando la relativa stringa di codice sulla piattaforma *twitter*.
Tale comportamento è espressione della c.d. "etica" della comunità dell'*hacking* e comporta, quantomeno nelle intenzioni del soggetto agente, il perseguimento di un interesse generale a vedere tutelati i dati informatici degli utenti della rete, anche sotto il profilo della *privacy*; siffatta consuetudine, peraltro, appare consolidata a tal punto che numerose aziende del settore hanno persino un'apposita sezione *on-line* dedicata alla ricezione delle segnalazioni di "errore", sezione che talora prevede addirittura premi economici per chi dia il proprio contributo alla sicurezza informatica del sistema[24].

[24] Tra i tanti, Neflix (società statunitense operante nella distribuzione di film o serie televisive attraverso lo *streaming*) nella sezione *web* dedicata afferma: «riteniamo che la ricerca e la divulgazione responsabile a tema sicurezza ci aiutino a migliorare di continuo le nostre procedure per tenere al sicuro abbonati, *partner* e dipendenti. Segnala potenziali vulnerabilità per la sicurezza tramite il nostro programma *Bug Bounty Bugcrowd*».

È indubbio, tuttavia, che la condotta appena descritta costituisce di per sé accesso abusivo a sistema informatico o telematico, quantomeno dal punto di vista oggettivo.
Conforto in tal senso giunge anche dalla giurisprudenza di merito: recentemente il Tribunale di Catania[25], ufficio del Giudice per le indagini preliminari, è stato investito della questione che si riassume brevemente di seguito.
La società L., produttrice di un'applicazione per *smartphone*, sporgeva denuncia-querela nei confronti di un *hacker* per accesso abusivo ad un sistema informatico e per diffamazione: la persona querelata aveva ottenuto dall'azienda diverse informazioni tecniche sul nuovo programma messo da poco in commercio e aveva iniziato un massiccio attacco nei confronti del *software*.
Dopo tale attività, l'*hacker* inviava diverse *e-mail* alla società titolare del programma, informandola dell'esistenza di una vulnerabilità di sistema e indicando precisamente dove si trovasse il *bug* da risolvere.
La società produttrice, tuttavia, non provvedeva a dare riscontro all'*hacker*, il quale, trascorso il termine ritenuto congruo dalla prassi della *cyber-community*, procedeva a pubblicare *on line* la stringa inerente al difetto dell'applicazione e le ulteriori fragilità riscontrate nel compimento dell'incursione.
Veniva così presentata una denuncia-querela nei confronti del soggetto in questione, per il reato di accesso abusivo a un sistema informatico o telematico.
A seguito della richiesta di archiviazione formulata dal Pubblico Ministero e della relativa opposizione proposta, il Giudice per le indagini preliminari riteneva di confermare l'infondatezza della notizia di reato, riconoscendo il valore, per così dire, "etico" della divulgazione responsabile.
Il Giudice, nel decreto di archiviazione, rilevava come l'*hat* «si [fosse] deciso a render noto, a tutela dei consumatori, la presenza di un simile errore a distanza di un mese dalla sua segnalazione; che la condotta dell'indagato non integra pertanto, sulla scorta di quanto chiarito, il delitto di cui all'art. 615-*ter* c.p., inquadrandosi la stessa nella metodologia comune della "divulgazione responsabile", avendo peraltro l'indagato medesimo contattato prima l'azienda coinvolta, proprio per consentirle di emendare l'errore entro un lasso di tempo, che può variare da trenta giorni a un anno, a seconda della gravità e della complessità della vulnerabilità».

[25] Trib. Catania, Uff. Gip, decreto 19 luglio 2019 in *www.giurisprudenzapenale.it*.

Secondo quanto affermato da alcuni autori, il Giudice catanese avrebbe dato piena rilevanza al comportamento successivo al fatto, rispetto a quanto compiuto nella consumazione del fatto stesso; pertanto, la motivazione "etica" e un ipotetico interesse meritevole di tutela avrebbero in qualche modo inciso sotto il profilo dell'antigiuridicità oppure sull'elemento psicologico[26] del dolo generico, determinando l'implicita irrilevanza penale del fatto. Secondo una terza soluzione interpretativa, la "divulgazione responsabile" sarebbe invece un elemento capace di influire sull'illiceità speciale, significata dall'avverbio "abusivamente" presente nell'art. 615-*ter* c.p.[27]
A fronte di tale decisione di merito, non sembra peregrino affermare che il predetto giudice per le indagini preliminari ha tentato di sopperire ai limiti della norma, cercando di ri-bilanciare il conflitto intersoggettivo di interessi codificato nella struttura della fattispecie[28]: i profili di giudizio hanno riguardato aspetti di carattere "privato" e quelli di interesse "collettivo", rispettivamente consistenti, per il primo, nelle prerogative del soggetto passivo a preservare da terzi lo spazio virtuale e a tutelare i dati in esso contenuti e, per il secondo, nell'interesse diffuso[29] alla sicurezza informatica dei servizi e della rete[30]. Tale scelta, che può essere opinabile sotto il profilo della scienza giuridica, sembra dimostrare i limiti esibiti dall'art. 615-*ter* c.p., a fronte dell'evoluzione tecnologica e delle nuove sfide informatiche future.

5. Tentativi dogmatici di inquadramento. Alla luce di quanto sin qui esposto, pare opportuno tentare di inquadrare, sotto un profilo dogmatico, il comportamento tenuto dall'*hacker* nella già menzionata attività di c.d. "divulgazione

[26] Sul punto PEANO, *Hacking etico: la divulgazione responsabile di errori del sistema informatico non è mai reato?*, in *www.quotidianogiuridico.it*.
[27] Di parere favorevole FLOR, '*Etical hacker', assolti ma non troppo: le "zone grigie" del diritto penale*, in *agendadigitale.eu*, 2 ottobre 2020. Sul concetto di illiceità speciale cfr. MORGANTE, *L'illiceità speciale nella teoria generale del reato*, Torino, 2002.
[28] Cfr. SALVADORI, *L'accesso abusivo ad un sistema informatico o telematico, una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in PICOTTI, *Tutela penale della persona e nuove tecnologie*, Padova, 2013, 126 s.
[29] Sul concetto interesse diffuso vd. Cons. St., Ad. Plen., 24 aprile 2012, n. 7; Cons. Stato, ad. plen., 4 giugno 2011, n. 10 in *Deiure.it*; PETRILLO, *La tutela giurisdizionale degli interessi collettivi e diffusi*, Milano, 2005.
[30] Cfr. FLOR, '*Etical hacker', cit.*, secondo il quale «il concetto di *cybersecurity* non può essere concepito come una *comprehesive concept*, quale processo proattivo e reattivo volto proprio alla protezione ideale dell'interesse degli uomini e delle organizzazioni ad essere liberi da minacce, in specie da quelle al suo nucleo essenziale meritevole di tutela, la c.d. *CIA-Triad* (la triade riservatezza, integrità e disponibilità di sistemi, programmi, dati e informazioni), cui può collegarsi l'esigenza di protezione dell'affidabilità di sistemi informatici, reti, dati e informazioni ivi contenuti o tramite di essi trattati».

responsabile" (R.V.D.), analizzando l'azione de qua alla luce della disciplina penale vigente.
La R.V.D. può essere suddivisa in tre autonomi momenti cronologici:
i) il primo, destinato alla raccolta di informazioni in merito al *software* o alla piattaforma oggetto di attenzione da parte dell'*haker*;
ii) il secondo: l'"attacco" diretto alla ricerca di possibili *bug* del sistema;
iii) il terzo, nel caso emerga la predetta vulnerabilità, la comunicazione al produttore o all'utilizzatore dell'esistenza della fragilità, con l'intento di sollecitare quest'ultimo, affinché si adoperi per la soluzione del problema.
Potrebbe, inoltre, esserci un ulteriore sviluppo fattuale, nel caso in cui la segnalazione non sia presa in considerazione dal proprietario del programma, e il "pirata informatico", in ossequio alla citata "etica" della comunità cybernauta, decida per mezzo dei *social* di divulgare la presenza di una fragilità in quel sistema.
Ovviamente, se la condotta si arresta allo stadio sopra descritto sub i), la medesima non presenterà alcuna rilevanza penale, trattandosi di mera attività preparatoria, di raccolta di informazioni, totalmente inidonea a mettere in pericolo il bene tutelato e ad integrare il fatto tipico.
Invece, l'azione sopra indicata sub ii) può astrattamente rientrare all'interno della fattispecie incriminatrice *ex* art. 615-*ter* c.p. e, riguardo alla stessa, valgono le considerazioni sopra spese in merito ai differenti tipi di attacco informatico (c.d. "porta chiusa a chiave", "porta chiusa ma non a chiave", "porta socchiusa").
Tuttavia, la peculiarità della "divulgazione responsabile" consiste nel fatto che il soggetto agente pone in essere gli atti preparatori e l'effettivo accesso al sistema informatico allo scopo di passare, poi, alla fase sopra descritta sub iii), vale a dire la comunicazione al produttore o all'utilizzatore dell'esistenza della fragilità, con l'intento di sollecitare quest'ultimo affinché si adoperi per la soluzione del problema.
Si tratta pertanto di stabilire se tale ulteriore attività, cui tendono oggettivamente e teleologicamente i precedenti atti di accesso al sistema informatico, elida o meno la punibilità degli stessi, dal punto di vista dell'antigiuridicità, della tipicità oggettiva ovvero soggettiva, considerato che la condotta nel suo complesso risulta finalizzata non già a danneggiare *tout court* il sistema informatico "attaccato", bensì a tutelare la sicurezza dei fruitori del sistema e così, indirettamente, il titolare dello stesso.

Un primo percorso da seguire potrebbe essere quello di riconoscere al "divulgatore responsabile" una sorta di causa di giustificazione del "consenso dell'avente diritto" sotto le figure del "consenso putativo" o del "consenso presunto".
Quanto al consenso putativo, si potrebbe ipotizzare che il proprietario del software permetta indistintamente a tutti gli *hat* di testare la sicurezza della piattaforma utilizzando un attacco *hacker*, assenso talvolta persino dichiarato pubblicamente per mezzo di una pagina web dedicata alla politica della DVR. Il consenso potrebbe essere eventualmente subordinato al rispetto delle procedure operative eticamente condivise da parte della comunità dei pirati informatici (comunicazione della vulnerabilità e relativi termini): qualora venga rispettata tale condizione, il fatto di "divulgazione responsabile" potrebbe ritenersi coperto ex ante dal consenso dell'avente diritto.
In questa situazione si potrebbe supporre che il pirata informatico abbia erroneamente creduto sussistente l'adesione senza riserve alla divulgazione responsabile, in quanto prassi condivisa e accettata dal mondo informatico; la presenza del consenso (putativo) permetterebbe di scriminare o quantomeno scusare, alla luce di quanto disposto *ex* art. 59, ult. comma, c.p., l'accesso abusivo poiché, anche se vi fosse un errore determinato da colpa nel presupporre l'autorizzazione a compiere l'azione criminosa, è pacificamente assente nel codice una omologa fattispecie di matrice colposa.
Una diversa lettura dell'art. 50 c.p. potrebbe riguardare la valorizzazione di una diversa situazione, ossia l'ipotesi del "consenso presunto": in tal caso, l'agente è ben a conoscenza del fatto che l'avente diritto non ha prestato il proprio consenso ai tentativi di incursione che egli si dispone a compiere, ma questi lo avrebbe dato se fosse stato informato della situazione di fatto (l'esistenza, cioè, di una vulnerabilità nascosta e non conosciuta che metta in pericolo la sicurezza del sistema).
La condotta potrebbe essere, così, scriminata nella prospettiva di interpretare la stessa alla stregua della *negotiorum gestio*[31], laddove l'atto materiale (l'intrusione) sia realizzato nel precipuo interesse dell'avente diritto (come dimostra la comunicazione del bug riscontrato), poiché quest'ultimo versa, in senso relativo, *in absentia domini* (vale a dire nella persistente ignoranza in

[31] Il primo orientamento c.d. oggettivistico trae elaborazione dalla dottrina tedesca nei primi anni del Novecento e, all'evidenza, si fonda sulla traslazione dell'istituto di natura civilistica contenuto nei paragrafi 677-684 *BGB* (cfr. ROSEMBERG, '*Strabrareiteilungen*', in *Gerichtsaal*, 62, 1903, Bd. I, 73 ss.; Von Hippel, *Manuale di diritto penale ('Lehrbuch des Strafrechts')*, Napoli, 1936, 174 ss.), così BELLAGAMBA, *I problematici confini della categoria delle scriminanti*, Milano, 2007, 78 e nt. 198.

merito alla vulnerabilità del sistema); d'altra parte, la ratio dell'istituto ex art. 2028 c.c. non mira solo a tutelare l'interesse individuale del singolo, ma anche al beneficio percepito dall'intera collettività grazie all'intervento volontario[32].

Un secondo percorso ermeneutico potrebbe fare leva sulla già menzionata clausola di illiceità speciale contenuta nell'art. 615-*ter* c.p. – cfr. l'avverbio «abusivamente»[33] – la quale, secondo l'opinione dominante, esclude l'operatività della causa di giustificazione di cui all'art. 50 c.p.[34]: in tali casi, infatti, la condotta priva di autorizzazione è elemento tipico negativo per la sussistenza della responsabilità penale (il c.d. consenso improprio).

Interpretando in senso soggettivo la medesima, è possibile sostenere che una condotta di accesso ad un sistema informatico, pur non espressamente acconsentita ma sorretta dalla convinzione di agire al fine preservare la sicurezza dei dati nel cyberspazio, sia sprovvista del carattere dell'abusività.

Qualora, dunque, si interpreti l'avverbio "abusivamente" nel senso di un c.d. "consenso improprio", i motivi a delinquere possono incidere sulla percezione del fatto concreto da parte del soggetto agente: ciò condurrebbe a un errore-motivo capace di escludere la perfetta conformità del fatto concreto, siccome rappresentato nella mente del soggetto agente, rispetto a quanto previsto dalla fattispecie astratta.

Laddove poi si interpreti la "clausola di illiceità speciale" quale «elemento positivo negativamente costruito dal legislatore»[35], consistente nella consapevo-

---

[32] P. GALLO, *voce Gestione d'affari altrui*, in *Dig.*, Agg., 424.

[33] Secondo alcuni autori il richiamo operato dal legislatore con l'espressione in parola sarebbe del tutto superfluo e non aggiungerebbe nulla sotto il profilo interpretativo, poiché utilizzato al solo fine di attivare l'attenzione del precetto, complessivamente inteso, sull'antigiuridicità della condotta (cfr. PIERGALLINI, *I delitti contro la riservatezza informatica*, in *Delitti contro la persona*, a cura di Piergallini, Viganò, Vizzardi, Verri, Padova, 2015, 770 ss.). Inoltre, la stessa Corte di Cassazione ha criticato la locuzione «abusivamente si introduce» per la «sua forte ambiguità e la conseguente possibilità d'imprevedibili e pericolose dilatazioni della fattispecie penale se non intesa in senso di "accesso non autorizzato" (v. Cass., Sez. V, 17 gennaio 2008, n. 2534; Cass., Sez. V, 3 luglio 2008, n. 26797; Cass., Sez. VI, 21 ottobre 2008, n. 39290, citate da SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *MediaLaws*, 2/2018, 3 nt. 2.

[34] Il carattere ambivalente dell'istituto del "consenso dell'avente diritto" è oggetto d'indagine e di dibattito nella dottrina sia italiana sia tedesca: da un lato, il consenso esclude la sussistenza del reato, qualora il delitto preveda che il fatto tipico si realizzi contro la volontà della vittima; dall'altro, la causa di giustificazione *ex* art. 50 c.p. elide l'antigiuridicità quando essa è diretta a rendere lecito ciò che è colpevole e conforme alla tipicità (cfr. ROXIN, '*Über die mutmaßliche Einwilligung*', in '*Festschrift für Hans Welzel*', Berlin-New York, 1974, tradotto in lingua italiana da CAVALIERE, *Sul consenso nel diritto penale*, in *Antigiuridicità e cause di giustificazione*, a cura di Roxin, Moccia, Napoli 1996, 87 ss.).

[35] V. CARNELUTTI, *Teoria generale del reato*, Padova, 1933, 53 ss.; M. GALLO, *Diritto Penale Italiano. Appunti di Parte Generale*, vol. I, Torino, 2019, 287 s.

lezza della mancanza di autorizzazione richiesta dalla tipicità, l'errore sul fatto nell'ambito della summenzionata "*responsible disclosure*" influirebbe, anche in questa diversa ricostruzione, sul processo motivazionale e volitivo a delinquere, sotto il profilo dell'elemento psicologico, tanto da escludere il dolo ai sensi dell'art. 47, comma 1, c.p.

Alla luce di quanto sin qui illustrato, la prassi della c.d. "divulgazione responsabile" sembra operare sì sul piano dei "motivi a delinquere" ma contestualmente risulterebbe escludere l'attributo della "abusività" della condotta.

A tal proposito, tuttavia, è opportuno rammentare che, secondo la *communis opinio*, ai fini della sussistenza del dolo di delitto, il nostro ordinamento non si preoccupa di indagare il concreto processo motivazionale che abbia portato l'agente alla condotta antidoverosa, rimanendo insensibile a tutti quegli aspetti "ispiratori" che lo abbiano guidato alla realizzazione del fatto tipico[36]. In tale prospettiva, la valutazione dei motivi a delinquere in sede di accertamento del fatto condurrebbe a difficoltà di non poco momento, poiché in ogni azione delittuosa vi sono presumibilmente motivi soggettivi che abbiano posto nel nulla l'efficacia dissuasiva della norma penale, come osservato da autorevole Dottrina[37].

6. *De iure condendo*. In conclusione, a fronte degli elementi proposti e delle criticità riscontrate, pare non più rinviabile, da parte del legislatore, una radicale revisione della fattispecie incriminatrice in parola, mediante il suo adeguamento al più aggiornato stato tecnico-scientifico della comunità dei cybernauti.

Siamo ben consapevoli che le più avanzate tecniche di *hacking* oggi in circolazione superano di gran lunga l'immaginazione degli studiosi e dello stesso legislatore[38]; tuttavia, *de iure condendo*, la struttura della figura delittuosa *de qua* potrebbe essere organizzata in più commi contenenti autonome fattispecie di reato a tutela di diversi bene giuridici.

---

[36] Cfr. PALAZZO, *Corso di diritto penale*, Torino, 2021, 455.

[37] Di tale opinione PALAZZO, *Corso*, cit., 456.

[38] Mi riferisco agli attacchi che utilizzano il c.d. *social engineering*, quali quello di *phishing*. I pirati informatici hanno rivoluzionato questa tecnica approdando al *Vishing*, ossia essa «si verifica quando un truffatore crea un sistema vocale automatizzato (o manuale) per fare chiamate vocali verso utenti telefonici e chiedere loro informazioni private. L'intento è lo stesso del *phishing* di *e-mail* o dell'SMS *phishing* (*smishing*): la chiamata vocale crea un senso di urgenza per l'utente che per questo motivo fornisce informazioni riservate» (così ROCCHI, *Il 'vishing' e la truffa del "consenso rubato": cos'è e come difendersi dal 'phishing' vocale*, in *www.cybersecurity360.it*) con cui accedere ai conti correnti delle vittime e impossessarsi del loro denaro.

Sotto il profilo della tipicità, l'elemento che richiederebbe maggiore precisazione è il concetto di "misure di sicurezza", quale presupposto della violazione. Gli obblighi di tutela di un sistema e le accortezze difensive richieste devono essere calibrate in ragione del ruolo svolto dall'utente: ad esempio, per un computer domestico è plausibile considerare sufficienti l'adozione di una semplice *password* con *antivirus*, ma non per un'azienda che propone un servizio in cui circolano dati di milioni di utenti.
Su punto, si tenga in considerazione il Regolamento 679/2016 (GDPR), che impone al Titolare del trattamento dei dati personali di predisporre misure idonee e capaci a proteggere queste informazioni; a tal proposito, il piano organizzativo per la sicurezza deve essere congegnato in ossequio a una valutazione dei «rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche» (art. 24)[39].
Da questo punto di vista, sarebbe forse opportuno operare un distinguo quanto all'esigibilità della condotta in relazione alla tipologia di utente: al semplice cittadino non possono, infatti, richiedersi le attenzioni e le competenze di cui devono necessariamente disporre, di contro, professionisti e aziende.
Da ultimo, in ragione della casistica e degli scopi per cui si compie la violazione di un calcolatore, l'elemento soggettivo, ora costituito dal dolo generico, potrebbe essere modificato in dolo specifico come il fine di profitto o di danno ingiusto[40]: con tale opzione legislativa, infatti, verrebbero perseguite solo quelle azioni che siano effettivamente mosse da intenti "criminali", escludendo dalla rilevanza penale condotte come la "divulgazione responsabile", e senza dover ricorrere sul piano dogmatico a scriminanti non codificate ovvero alla controversa clausola di illiceità speciale.

[39] La dottrina attribuisce al concetto di "rischio" due distinte accezioni: la prima, "rischio inerente" «fa riferimento al rischio che una attività di trattamento di dati personali incorpora prima che il titolare abbia considerato le misure di sicurezza o altri fattori di mitigazione che sono stati posti in essere»; la seconda, "rischio residuale" riguarda il «rischio per i diritti e le libertà degli interessati che è considerato al netto dell'effetto di mitigazione sortito dalle misure di sicurezza e dai meccanismi di controllo adottati dal titolare», così SANTORO, *Le misure di sicurezza adeguate e l'analisi del rischio*, (a cura di) PERRI-ZICCARDI, *Tecnologia e diritto. Informatica Giuridica 'Data governance', protezione dei dati e GDPR*, vol. 2, Milano, 2019, 103 s.

[40] Sulle tematiche del dolo specifico con il principio di offensività e il problema legato al disvalore penalmente sanzionato, cfr. MARINO, *Il "filo di Arianna". Dolo specifico e pericolo nel diritto penale della sicurezza*, in *Dir. pen. cont.*, 6/2018, 41 ss.; PICOTTI, *Il dolo specifico. Un'indagine sugli elementi finalistici' delle fattispecie penali*, Milano, 1993, 501 s.