PRIME NOTE IN MATERIA DI "DDL CYBERSICUREZZA" APPROVATO (IN VIA DEFINITIVA) IN DATA 19 GIUGNO 2024: QUANDO IL RIMEDIO PUÒ DIVENTARE PEGGIORE DEL MALE

1. Premessa

Il 19 giugno 2024 è stato approvato in via definitiva il c.d. "DDL Cybersicurezza" (di seguito anche solo "DDL"): atto normativo con cui l'Italia vorrebbe apprestarsi a compiere un più concreto passo verso il contrasto al c.d. *cybercrime*. La nuova legge, recante "*disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*", si pone così in linea con gli indirizzi europei in materia di sicurezza informatica e rappresenta un'anticipazione del nostro Paese degli obblighi di recepimento della Direttiva (UE) 2022/2555 sulla sicurezza delle reti e delle informazioni (cd. Direttiva NIS 2)[1].

Lo scopo del provvedimento vorrebbe essere quello di fornire risposta all'allarme generato dai crescenti attacchi informatici subiti da imprese e pubbliche amministrazioni ed in specifico, attacchi di tipo *ransomware*[2] o DDoS (*Distributed Denial of Service*)[3]. A tal fine, l'articolato richiede alle entità pubbliche ritenute più a rischio di adottare "sistemi di cybersicurezza" e di segnalare tempestivamente gli attacchi eventualmente subiti (da un lato) e introduce modifiche processuali e sostanziali al fine di aggravare il trattamento sanzionatorio e rendere più agevole l'accertamento dei c.d. *cybercrime* (dall'altro). Due direzioni che da subito fanno dubitare che la strada imboccata possa essere quella davvero risolutiva e non aggravatrice del male che pur si vorrebbe giustamente sconfiggere.

2. Le previsioni in materia di organizzazione delle pubbliche amministrazioni

Il Capo I (artt. 1-15) del DDL reca intanto disposizioni volte al rafforzamento delle Pubbliche Amministrazioni di fronte a possibili attacchi informatici. In specifico, il

[1] Direttiva (UE) 2022/2555.

[2] SCARAMELLINI, "Cyber attack, reati informatici e patrimonio aziendale", in "La tutela penale del patrimonio aziendale – rilevanza penale degli asset intangibili e strumenti di tutela", (a cura di) STAMPANONI BASSI, Bologna, I ed., 2023, pag. 490: "[…] ransomware*, ovverossia* virus *malevoli in grado di bloccare un dispositivo 'sequestrando' i dati ivi contenuti* […]".

[3] Siffatti *malware* agiscono bloccando l'accesso ai dati vitali delle organizzazioni, per poi richiedere un riscatto per la relativa riattivazione. Del pari, gli attacchi tipo DDoS costituiscono un'altra perniciosa minaccia dal momento che, prendendo di mira l'intera infrastruttura di una rete mediante sovraccarico dei relativi servizi, la rendono del tutto inoperabile.

Legislatore sembra aver preso atto che il 41% degli attacchi informatici perpetrati in Italia risulta diretto contro le amministrazioni statali[4]: indice di una chiara inefficacia delle barriere informatiche oggi implementate dalle PA per difendersi dai *cybercriminali*.

Al fine di colmare siffatto *gap* sulle Pubbliche Amministrazioni[5] viene dunque posto:

- *ex ante*, un obbligo di adozione di misure di sicurezza, procedure e protocolli idonei a prevenire attacchi informatici;

- *ex post*, un obbligo di attivarsi tempestivamente per salvaguardare il più possibile la riservatezza dei dati personali e delle informazioni detenute ed oggetto dell'eventuale attacco informatico.

Più in dettaglio: sulla "falsariga" dell'ormai noto modello introdotto dal Regolamento Europeo n. 2016/679 (GDPR) in materia di protezione dei dati personali, con l'articolo 1 del DDL si introduce in capo alle Pubbliche Amministrazioni l'obbligo di segnalazione e notifica all'Autorità Nazionale per la Cybersicurezza ("ACN") di tutti gli incidenti "*aventi impatto su reti, sistemi informativi e servizi informatici di rispettiva pertinenza*" (ossia di tutti gli incidenti già contemplati dalla disposizione di cui all'art. 1, comma 3-bis, D.L. n. 105/2019[6]) entro 24 ore dal momento in cui ne siano venute a conoscenza.

Il medesimo articolo 1 delinea quindi modalità e tempi con cui operare la segnalazione, introducendo poi apposite sanzioni in caso di violazione dell'obbligo. Segnatamente, a seguito di un primo inadempimento all'obbligo di comunicazione, la Pubblica Amministrazione potrà ricevere una comunicazione preliminare da parte dell'ACN contenente l'avvertenza che, in caso di una nuova inosservanza, commessa entro 5 anni, sarà soggetta all'irrogazione delle sanzioni previste al successivo comma 6 dell'art. 1 e ricomprese tra un minimo di 25.000 euro ed un massimo di 125.000 euro. In ogni caso, entro 12 mesi dal primo Avviso l'ACN potrà disporre ispezioni volte a verificare che l'Ente interessato abbia nelle more adottato misure di effettivo rafforzamento della propria struttura cibernetica secondo quanto prescritto dalla stessa ACN o dalle linee

[4] Il Sole24ore: https://ntplusentilocaliedilizia.ilsole24ore.com/art/enti-pubblici-alert-azioni-cybercriminali-le-commesse-pnrr-AF4eT1TC.

[5] Con ciò vanno intese: le amministrazioni dello Stato; le società in house che forniscono servizi informatici, i servizi di trasporto di cui al primo periodo dell'articolo 1 della Legge in commento ovvero servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991, o di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008; le Regioni e gli enti locali; le provincie autonome; i comuni con popolazione superiore a 100 mila abitanti; i capoluoghi di regione; le società di trasporto pubblico urbano con utenza non inferiore a 100 mila abitanti e le ASL.

[6] D. L. del 21 settembre 2019, n. 105, recante "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*".

guida di settore. Sicché è chiara la prospettiva: se vieni "bucato" la colpa è essenzialmente tua.

Bene quindi precisare che, ai sensi dell'art. 7 del DDL, i predetti obblighi di segnalazione non si applicano:

- agli operatori di servizi essenziali ed ai fornitori di servizi digitali contemplati dall'art. 3, comma 1, D.lgs. n. 65/2018[7] (cd. soggetti NIS);

- ai soggetti già inclusi nel c.d. "perimetro di sicurezza nazionale cibernetica" ai sensi dell'art. 1, commi 2, lett. a), e 2-bis, D.L. n. 105/2019;

- agli organi dello Stato preposti alla prevenzione, all'accertamento ed alla repressione dei reati, alla tutela dell'ordine e della sicurezza pubblica ed alla difesa e sicurezza militare dello Stato ed agli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 Legge n. 3 agosto 2007, n. 124.

Ne risulta manifesta la volontà del Legislatore di assicurare un ruolo centrale all'Autorità Nazionale per la Cybersicurezza ACN a cui vengono infatti attribuiti poteri tanto ispettivi quanto sanzionatori, secondo una tendenza che trova più espressa conferma al successivo art. 2 del DDL, laddove prevede che le indicazioni fornite dall'ACN alle Pubbliche Amministrazioni abbiano carattere perentorio (da un lato) e che la mancata ottemperanza delle PA alle stesse indicazioni possa comportare l'applicazione delle già richiamate sanzioni (da 25.000 a 125.000 euro) di cui all'art. 1, comma 6 del DDL (dall'altro).

Sotto altro profilo il DDL si prefigge di operare una modernizzazione tecnologica delle Pubbliche Amministrazioni, introducendo cioè il dovere di creare una struttura (anche individuandola tra quelle già esistenti) preposta alla specifica attività di cybersicurezza; nonché, di istituire la figura di "Referente per la cybersecurity", ossia un soggetto deputato a fungere da "cinghia di trasmissione" tra il singolo Ente Pubblico e l'Autorità Nazionale per la Cybersicurezza.

3. Modifiche al Codice penale

Accanto al piano della riorganizzazione amministrativa si pongono le modifiche alle fattispecie di reato intese a contrastare più efficacemente il fenomeno della *cybercriminalità*. In particolare, con l'articolo 16 del DDL, rubricato "*Modifiche al Codice Penale*", il Legislatore è intervenuto: (i) introducendo nuove ipotesi di reato; (ii) innalzando le pene di alcuni reati già previsti nel Codice penale; (iii) ampliando i confini

[7]D. Lgs. 18 maggio 2018, n. 65, volto alla "*Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*".

del dolo specifico di alcune fattispecie e (iv) introducendo nuove circostanze aggravanti ed attenuanti.

In via segnata, il primo intervento riformatore ha interessato la fattispecie di "*Accesso abusivo ad un sistema informatico o telematico*" di cui all'art. 615-*ter* c.p., prevedendosi un aumento della cornice edittale:

- da 2 a 10 anni di reclusione per le ipotesi disciplinate dal comma 2:
    - fatto commesso "*da pubblico ufficiale/incaricato di pubblico servizio, con abuso di poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato o con abuso della qualità di operatore del sistema*");
    - fatto commesso con "*violenza sulle cose o alle persone*" o da soggetto "*palesemente armato*";
    - se dal fatto deriva "*la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento, dei dati, delle informazioni o dei programmi in esso contenuti*".

- da 3 a 10 anni e/o da 4 a 12 anni per l'ipotesi in cui i reati di accesso abusivo ad un sistema informatico o telematico (nelle forme "semplice" di cui al comma 1 od "aggravata" di cui al comma 2) riguardi"*sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico*".

Oltre ad intervenire sulle cornici edittali, il Legislatore è poi intervenuto altresì sulla formulazione della fattispecie:

- al comma 2 n. 2, affiancando all'aggravante della "*violenza sulle cose o alle persone*" quella del fatto commesso con "*minaccia*" ed al

- comma 2 n. 3 aggiungendo all'aggravante del "*danneggiamento dei dati delle informazioni o dei programmi in esso contenuti*" quella della loro "*sottrazione, anche mediante riproduzione o trasmissione, o [relativa] inaccessibilità da parte del titolare*".

Le modifiche che intervengono in merito alla fattispecie che sanziona la "*detenzione, diffusione, e istallazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*" (art. 615-*quater* c.p.), non sono per nulla dissimili. Invero, anche in siffatta fattispecie, si procede sia con l'aggravamento della cornice

edittale in seguito al verificarsi di determinate circostanze (che sono peraltro quelle contenute nell'art. 615-*ter c.p.*) sia con l'espansione della fattispecie astratta.

Sul fronte delle circostanze:

- il comma 2 prevede ora la reclusione da due a sei anni "*quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1)*", mentre,

- il comma 3 stabilizza la pena della reclusione dai tre agli otto anni "*quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma*".

Sul fronte del *corpus* della disposizione, si prevede adesso una nuova formulazione, in quanto:

- al primo comma, il fine del dolo specifico del "*profitto*" viene sostituito con quello, sicuramente più generico, del "*vantaggio*".

È bene però sottolineare che più disposizioni seguiranno la scia tracciata dal 615-*ter*. Infatti, il DDL, in seguito alla modifica del 615-*quater* ed alla ricollocazione della fattispecie *ex* 615-*quinquies* c.p. (ora abrogata) nel novero dei delitti di danneggiamento (nello specifico, all'interno dell'art. 635-*quater*.1 c.p.), procede pedissequa con l'irrigidimento delle pene sulla scorta sempre del 615-*ter*.

A riprova di ciò, basti guardare al delitto di cui all' art. 617-*bis* c.p. "*detenzione, diffusione e istallazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche*", che viene arricchito con un secondo comma identico a quello contenuto nell'art- 615-*quater*.

Riconferma di siffatta tendenza sia anche la modifica prevista per la disposizione di cui all'articolo 617-*quater* c.p. relativo al delitto di "*intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*".

Anche qui si assiste infatti al:

- sensibile aumento della cornice edittale per le circostanze aggravanti di cui al comma 4 (da 4 a 10 anni, in luogo della precedente da 3 ad 8) ed alla

- rimodulazione ed estensione delle stesse; imponendo, in particolare, la procedibilità *ex officio* ed il predetto aumento sanzionatorio qualora il fatto venga commesso:

- "*in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615-ter, terzo comma*" oppure

- "*in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso delle qualità di operatore del sistema*"

Chiara quindi l'influenza dell'art. 615-*ter* c.p. nella riformulazione anche di siffatta norma.

A sua volta, l'articolo 617-*quater* c.p. viene richiamato dalla disposizione immediatamente successiva, ossia l'articolo 617-*quinquies*, relativa al delitto di "*detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere, comunicazioni informatiche o telematiche*". Se, tuttavia, prima dell'entrata in vigore della normativa in esame, l'art. 617-*quater*, quarto comma, veniva menzionato per giustificare una generica estensione della cornice edittale (la reclusione da 1 a 4 anni diveniva invero da 1 a 5), adesso opera una *distinctio* nel regime sanzionatorio in base alla circostanza che andrà ad integrarsi nel caso concreto. Invero:

- nel caso in cui dovesse sussistere l'aggravante del quarto comma, numero 1), la pena sarebbe "*della reclusione da tre a otto anni*";

- qualora dovesse risultare, invece, integra l'ipotesi di cui al quarto comma, numero 2), la reclusione diventerebbe "*da due a sei anni*".

Da ultimo, la pena diventa "*della reclusione da tre a otto anni*" (e non più da uno a cinque) anche per il delitto disciplinato dall'art. 617-*sexies* c.p., rubricato "*falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche*", pure qui a seguito del verificarsi di una delle circostanze aggravanti ad efficacia speciale previste dall'art. 617-*quater*.

Nondimeno, la Legge introduce anche due nuove circostanze attenuanti.

É parso infatti opportuno controbilanciare il predetto irrigidimento sanzionatorio appena delineato con delle previsioni che "strizzino l'occhio" a favore degli autori di fatti considerabili di lieve entità o di chi collabori con l'autorità giudiziaria e con le forze di polizia al fine di evitare che l'attività delittuosa porti a conseguenze ulteriori.

La nuova disposizione di cui all'articolo 623-*quater* c.p. prevede invero:

- al primo comma che "*le pene comminate per i delitti di cui agli articoli 615*-ter*, 615*-quater*, 617*-quater*, 617-quinquies e 617*-sexies *sono diminuite quando, per la natura, la specie, i mezzi, le modalità o circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità*". Si ripropone per tal evenienza il noto schema della circostanza attenuante per particolare tenuità del fatto, già presente nel nostro codice (ad esempio) per i delitti contro la personalità dello Stato (v. art. 311 c.p.[8]);

- al secondo comma che "*Le pene previste per i delitti di cui al primo comma sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi*". In sostanza, condotte di collaborazione *post delictum*, volte tanto a limitare i danni quanto a un'efficace attività di individuazione dei possibili responsabili secondo una soluzione non certo inedita, ma già introdotta (e talvolta con profitto) in altri settori dell'ordinamento penale (ad esempio per i delitti contro la fede pubblica[9]);

- al terzo comma, al manifesto fine di massimizzare l'applicazione delle nuove attenuanti di cui sopra, è altresì chiarito che "*non si applica il divieto di cui all'articolo 69, quarto comma*". Le attenuanti di cui al comma 1 e comma 2 vengono così sottratte al divieto di prevalenza sulla recidiva reiterata e sulle altre circostanze ivi richiamate[10].

Le medesime peculiarità caratterizzano poi anche la nuova attenuante *ex* art. 639-*ter* c.p., che opera con riferimento ai delitti di cui agli artt. 629, terzo comma, 635-*ter*, 635-*quater*.1 e 635-*quinquies*. Si ripropongono dunque le stesse considerazioni compiute per

---

[8] La disposizione di cui all'art. 311 c.p. prevede che "*Le pene comminate per i delitti preveduti da questo titolo sono diminuite quando per la natura, la specie, i mezzi, le modalità o circostanze dell'azione, ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità*".

[9] La disposizione di cui all'art. 474-*quater* c.p. prevede che "*Le pene previste dagli articoli 473 e 474 sono diminuite dalla metà a due terzi nei confronti del colpevole che si adopera per aiutare concretamente l'autorità di polizia o l'autorità giudiziaria nell'azione di contrasto dei delitti di cui ai predetti articoli 473 e 474, nonché nella raccolta di elementi decisivi per la ricostruzione dei fatti e per l'individuazione o la cattura dei concorrenti negli stessi, ovvero per l'individuazione degli strumenti occorrenti per la commissione dei delitti medesimi o dei profitti da essi derivanti*".

[10] La disposizione di cui all'art. 69, comma 4 c.p. prevede che "*Le disposizioni del presente articolo si applicano anche alle circostanze inerenti alla persona del colpevole, esclusi i casi previsti dall'articolo 99, quarto comma, nonché dagli articoli 111 e 112, primo comma, numero 4), per cui vi è divieto di prevalenza delle circostanze attenuanti sulle ritenute circostanze aggravanti, ed a qualsiasi altra circostanza per la quale la legge stabilisca una pena di specie diversa o determini la misura della pena in modo indipendente da quella ordinaria del reato*".

l'articolo precedente in merito alla rigidezza sanzionatoria ed al contestuale tentativo di mitigare siffatta spinta repressiva.

Poi, proprio per la specifica gravità e frequenza delle condotte criminose perpetrate a mezzo di strumenti informatici, sono state introdotte dal testo in esame figure di reato propriamente informatiche, quali (ad esempio) l'estorsione informatica (art. 629, comma 3, c.p.): "*chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità*".

Per questa nuova tipologia estorsiva si commina la sanzione della reclusione dai 6 ai 12 anni e la multa da 5.000 a 10.000 euro a chiunque costringa taluno a fare od omettere qualche cosa, procurando a sé o altri un ingiusto profitto con altrui danno, mediante:

- accesso abusivo ad un sistema informatico o telematico;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche;
- danneggiamento di informazioni, dati e programmi informatici e di sistemi informatici o telematici di pubblica utilità (o meno).

La pena si aggrava ulteriormente, innalzandosi la cornice edittale per la reclusione da 8 a 22 anni e la multa da 6.000 a 18.000 euro, nel caso in cui concorra una delle circostanze indicate nel terzo comma dell'articolo 628 c.p. oppure qualora la persona offesa sia persona incapace per età o per infermità.

Vengono poi apportate delle modifiche pressocché identiche a quelle già accennate per alcuni articoli relativi a varie ipotesi di danneggiamento (635-bis c.p., 635-quater c.p., 635-ter c.p., 635-quinquies c.p.). Per tutte le accennate disposizioni è infatti previsto un aumento delle soglie edittali e l'allineamento delle originarie circostanze aggravanti di ciascun articolo a quelle dettate con il nuovo art- 615-ter c.p.

Da ultimo, anche l'articolo 640 c.p. è stato soggetto a modifiche da parte della Legge in analisi:

- attraverso la previsione della nuova disposizione di cui al comma secondo, numero 2-ter viene introdotta un'ulteriore circostanza aggravante configurabile in tutti quei casi in cui il reato venga commesso profittando della distanza garantita dagli strumenti informatici o telematici utilizzati, così da ostacolare la "*propria o altrui identificazione*[11]";

- per fini di "ingegneria" legislativa, si è poi proceduto a modificare la formulazione del terzo comma del medesimo articolo, che non fa più menzione dell'espressione "*dal capoverso precedente*", ora recitando: "*il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal secondo comma, ad eccezione di quella di cui al numero 2-ter o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7*", e così prevedendo il regime di procedibilità a querela per la fattispecie di nuova introduzione.

Infine, sempre alla summenzionata ipotesi disciplinata dall'articolo 640, secondo comma, si applicherà la misura di sicurezza della confisca, poiché la Legge ha incluso nel dettato dell'art. 640-quater c.p., rubricato "*applicabilità dell'articolo 322-ter*[12]", anche il neo-introdotto numero 2-ter.

4. Modifiche al codice di procedura penale

Il diritto penale sostanziale non è il solo piano su cui il Legislatore mostra concrete intenzioni: sul piano processuale si fanno infatti ricondurre tutte le fattispecie di criminalità informatica più gravi nella disciplina dedicata ai cc.dd. reati di criminalità organizzata (artt. 51 e 407 c.p.p.), così da consentire il maggior utilizzo possibile di più

[11] In tal modo, si conferma la tendenza, più volte citata, di arginare le condotte delittuose poste in essere nell'ambiente digitale attraverso l'aggravamento della cornice edittale.

[12] La disposizione di cui all'art. 322-*ter* c.p. prevede che: "*Nel caso di condanna, o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale, per uno dei delitti previsti dagli articoli da 314 a 320, anche se commessi dai soggetti indicati nell'articolo 322 bis, primo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto o il prezzo, salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto. Nel caso di condanna, o di applicazione della pena a norma dell'articolo 444 del codice di procedura penale, per il delitto previsto dall'articolo 321, anche se commesso ai sensi dell'articolo 322 bis, secondo comma, è sempre ordinata la confisca dei beni che ne costituiscono il profitto salvo che appartengano a persona estranea al reato, ovvero, quando essa non è possibile, la confisca di beni, di cui il reo ha la disponibilità, per un valore corrispondente a quello di detto profitto e, comunque, non inferiore a quello del denaro o delle altre utilità date o promesse al pubblico ufficiale o all'incaricato di pubblico servizio o agli altri soggetti indicati nell'articolo 322 bis, secondo comma. Nei casi di cui ai commi primo e secondo, il giudice, con la sentenza di condanna, determina le somme di denaro o individua i beni assoggettati a confisca in quanto costituenti il profitto o il prezzo del reato ovvero in quanto di valore corrispondente al profitto o al prezzo del reato*".

penetranti (ma al contempo più invasivi) strumenti di indagine ed accertamento, al contempo ampliando altresì la competenza ed il coordinamento delle Direzioni distrettuali antimafia. Aspetto, quest'ultimo, che, se da un lato risponde all'esigenza di accertamento di indagini a fronte di reati che si consumano in uno spazio (territorialmente) indefinito e potenzialmente assai vasto, accentua e consolida anche un sistema basato su diversi e distinti "binari".

Le modifiche al codice di procedura sono introdotte dall'articolo 17 del disegno di legge approvato in via definitiva che (i) estende, in particolare, al catalogo dei reati informatici la competenza del procuratore distrettuale e (ii) espande la disciplina derogatoria di cui agli artt. 406 e 407 c.p.p. ai delitti in commento.

Quanto al primo dei menzionati profili innovativi, vengono ricomprese nel novero delle fattispecie sottoposte alla competenza del procuratore distrettuale:

- l'articolo 635-*quater.1*, "*detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema telematico*";

- l'art. 635-*quinquies*, "*danneggiamento di sistemi informatici o telematici di pubblico interesse*" ed

- il delitto di cui all'articolo 1, comma 11, del d.l. n. 105 del 2019.

Quanto al secondo elemento di novità, viene aggiunto all'articolo 407, comma 2, lettera a), c.p.p. un nuovo numero 7-ter, idoneo ad allungare il termine massimo di durata delle indagini preliminari a due anni nel caso in cui si proceda per delitti previsti dagli artt. 615-*ter*, 615-*quater*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 635-*quater.1* e 635-*quinquies* c.p. "*quando il fatto è commesso in danno di sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico*".
Siffatta disposizione viene ricompresa inoltre tra le deroghe disposte dall'art. 406, comma 5-*bis*, c.p.p. alla disciplina relativa alla notifica dell'avviso della richiesta di proroga delle indagini preliminari e di fissazione dell'udienza in camera di consiglio da parte del giudice per le indagini preliminari (beninteso, in caso di mancato accoglimento dell'istanza).

In aggiunta, il Codice di rito diviene destinatario di ulteriori modificazioni anche per via incidentale, ossia attraverso la modifica di alcune leggi speciali.

Invero:

- l'articolo 18 modifica tre disposizioni (art. 9, comma 2; art. 11, comma 2; art. 16-*nonies*, comma 1) del d.l. n. 8 del 1991, rubricato "*nuove norme in materia di sequestri di persona a scopo di estorsione e per la protezione dei testimoni di giustizia, nonché per la protezione e il trattamento sanzionatorio di coloro che collaborano con la giustizia*".

    - Il primo dei tre commi di cui sopra consente agli autori di reati informatici previsti al comma 4-*bis* dell'articolo 371-*bis* c.p.p. di beneficiare delle speciali misure di protezione riservate a coloro che abbiano svolto attività di collaborazione nell'ambito di un procedimento penale, rendendo dichiarazioni qualificate ai sensi del terzo comma del medesimo articolo[13].

    - Per gli stessi reati di cui al comma 4-*bis*, l'articolo 11 del già menzionato d.l. stabilisce che venga effettuata la comunicazione della proposta di ammissione alle suddette misure speciali di protezione al procuratore nazionale antimafia ed antiterrorismo.

    - L'art. 16-*nonies*, comma 1, del citato d.l. dispone che le persone condannate per i reati in esame che abbiano prestato, anche dopo la condanna, taluna delle condotte di collaborazione che consentono la concessione delle circostanze attenuanti previste dal Codice penale o da disposizioni speciali, godano dei benefici penitenziari riservati dalla legge ai soggetti che collaborano con la giustizia.

- L'art. 19 modifica a sua volta l'art. 13 del d.l. n. 152 del 1991, rubricato "*provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*". In particolare,

    - viene ivi inserito un nuovo comma 3-*bis*, che estende la disciplina delle intercettazioni prevista per i fatti di criminalità organizzata ai reati informatici enucleati all'articolo 371-*bis*, comma 4 *bis*, c.p.p.

- Da ultimo, l'articolo 21 del testo normativo in esame, modificando la Legge n. 6 del 2018, recante "*Disposizioni per la protezione dei testimoni di giustizia*", tende

[13] La disposizione di cui al comma 3 dell'articolo 9 decreto-legge n. 8 del 1991 prevede che "*Ai fini dell'applicazione delle speciali misure di protezione, assumono rilievo la collaborazione o le dichiarazioni rese nel corso di un procedimento penale. La collaborazione e le dichiarazioni predette devono avere carattere di intrinseca attendibilità. Devono altresì avere carattere di novità o di completezza o per altri elementi devono apparire di notevole importanza per lo sviluppo delle indagini o ai fini del giudizio ovvero per le attività di investigazione sulle connotazioni strutturali, le dotazioni di armi, esplosivi o beni, le articolazioni e i collegamenti interni o internazionali delle organizzazioni criminali di tipo mafioso o terroristico-eversivo o sugli obiettivi, le finalità e le modalità operative di dette organizzazioni*".

all'efficientamento dei rapporti tra l'ACN, il procuratore nazionale antimafia e antiterrorismo, la polizia giudiziaria ed il pubblico ministero. Si prevede infatti:

- un obbligo di immediata trasmissione delle notifiche di incidente da parte dell'Agenzia al Ministero dell'interno per la sicurezza e per la regolarità del servizio di telecomunicazione (disposizione funzionale a consentire al pubblico ministero di ricevere tempestivamente la notizia di reato);

- obblighi informativi nei confronti del Procuratore nazionale antimafia e antiterrorismo e, infine,

- gli obblighi gravanti sul pubblico ministero di dare tempestiva informazione all'Agenzia delle notizie di reato (delle quali sia edotto) relative ai delitti di cui all'art. 371-*bis*, comma 4-*bis* e di assicurare il raccordo informativo con il Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione.

5. Previsioni in materia di 231

Nemmeno le imprese rimangono esenti dall'*aggravio* sanzionatorio introdotto dalla normativa in commento, in quanto l'articolo 20 del nuovo testo di legge interviene nell'ambito della responsabilità amministrativa derivante da reato. In particolare, mediante la modifica dell'art. 24 *bis* del d. lgs. 231 del 2001:

- vengono innalzate le sanzioni di cui al primo comma (ora da duecento a settecento quote);

- viene inserito un nuovo comma 1-*bis*, che prevede l'applicazione di una sanzione pecuniaria da trecento a ottocento quote per l'ipotesi (di nuovo conio) di estorsione informatica di cui all'art. 629, terzo comma, c.p.;

- il riferimento all'art. 615-*quinquies* c.p. di cui al comma secondo viene sostituito con il richiamo al nuovo art. 635-*quater*.1 e le relative sanzioni pecuniarie derivanti dalla commissione di tale illecito vengono innalzate da trecento a quattrocento quote e

- da ultimo, si prevede che "*nei casi di condanna per il delitto indicato nel comma 1-bis si applicano le sanzioni interdittive previste dell'art. 9, comma 2, per una durata non inferiore a due anni*".

6. Conclusione

In conclusione, il "DDL Cybersicurezza" vorrebbe porsi come presidio del rischio generato dai cybercrimes operando su due fronti: innalzando le pene per i "carnefici" (da un lato) e responsabilizzando le vittime per il tramite di un "rinforzo" strutturale a queste ultime richiesto (*rectius*: imposto) (dall'altro).

Cionondimeno, se sul lato strutturale non si evidenziano particolari criticità, non si può ripetere identica affermazione sul lato più prettamente giuridico e di scelte legislative.

Il Legislatore aveva invero davanti a sé una (ed una sola) opzione: stanziare delle somme di denaro da destinare per il compimento di riforme volte in tal senso, e, invece, la strada che si è deciso di imboccare è stata quella di riportare alcune delle fattispecie sopra esaminate entro il novero dei cc.dd. reati di "criminalità organizzata", estendendo così loro la disciplina (maggiormente repressiva) prevista per siffatte categorie di reati.

Scelta che pare non condivisibile. Nonostante sia sicuramente vero che la Procura nazionale antimafia goda di maggiori risorse rispetto agli ordinari Uffici di Procura, la specificità di tali fattispecie imporrebbe infatti una trattazione *ad hoc*, per via (anche) della particolarissima *expertise* richiesta per contrastare il fenomeno. E sono queste specifiche *expertise* che andrebbero finanziate.

A fortiori, la prassi insegna (ad esempio) che l'istituto delle intercettazioni non agevola in alcun modo l'attività di individuazione dei "cybercriminali", che continuano ad operare nell'ombra restando, di conseguenza, impuniti, data la mancanza nel nostro Paese di attrezzature tecnologiche all'avanguardia (sicuramente molto costose) necessarie per una precisa identificazione di questi ultimi.

Da ultimo, queste nuove modifiche rischiano di dispiegare un solo effetto: aggravare le persone offese che divengono destinatarie di pressanti obblighi di segnalazione, la cui inosservanza comporterebbe l'irrogazione di pesanti sanzioni di natura amministrativa. Invece, per ciò che concerne i "carnefici", non sembra che l'attuale normativa di accertamento degli autori riesca a far fronte alle problematiche che i cc.dd. "crimini 2.0" pongono in essere (*in primis*, il problema derivante dalla possibilità di agire mascherando la propria identità in uno spazio virtuale pressocché infinito). Con la conseguenza che le vittime diventerebbero i soli carnefici perseguitati.

Detto in breve: una modifica legislativa operata con poca esperienza empirica rischia di portare al risultato del "cornuto e mazziato": i veri responsabili non saranno identificati e le sole responsabilità che si faranno valere saranno quelle di chi è stato "bucato". La guerra si vince non cedendo ai ricatti dei vari autori (che è molto difficile poter identificare) ed avendo dei sistemi di back-up molto efficienti che consentono di non dover subire i ricatti.