Sintetica illustrazione del "DDL Cybersicurezza", approvato dal Consiglio dei ministri nella seduta del 25 gennaio 2024.

In data 25 gennaio 2024, con l'approvazione da parte del Consiglio dei ministri del nuovo Disegno di Legge sulla cybersicurezza (a seguire, DDL), l'Italia ha compiuto un primo (pur iniziale) passo verso il contrasto al fenomeno del c.d. *cybercrime*. Trattasi di un inevitabile allineamento agli indirizzi europei, che vorrebbe rappresentare altresì un'anticipazione degli obblighi di recepimento della Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio sulla sicurezza delle reti e delle informazioni (cd. Direttiva NIS 2)[1].

Siffatto DDL risponde segnatamente alla crescente esigenza di poter efficacemente contrastare le gravi e invasive minacce derivanti da attacchi informatici attuati mediante (ad esempio) *virus* tipo *ransomware*[2] oppure attacco stile DDoS (Distributed Denial of Service)[3].

A questi fini, il DDL richiede alle entità ritenute più a rischio di adottare e/o implementare sistemi di cybersicurezza, nonché di segnalare tempestivamente gli attacchi eventualmente subiti.

Nondimeno, il disegno di legge è teso a garantire altresì una minore vulnerabilità delle pubbliche amministrazioni (soprattutto di quelle estranee al "Perimetro di sicurezza nazionale cibernetica"); ad incrementare la rilevanza dell'Agenzia per la cybersicurezza nazionale (ACN); a promuovere il coordinamento dell'attività di questa con l'Autorità giudiziaria; a consentire un immediato intervento dell'Agenzia a fini di prevenzione e di ripristino delle funzionalità dei sistemi informatici oggetto di attacco.

[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.

In particolare, alla Pubblica Amministrazione – con ciò dovendosi intendere le amministrazioni dello Stato, le rispettive società *in house*, 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 – viene imposta l'adozione di misure sicurezza, procedure e protocolli idonei a prevenire pericolose incursioni informatiche (*ex ante*); nonché ad attivarsi tempestivamente per salvaguardare il più possibile la riservatezza dei dati personali e delle informazioni detenute (*ex post*).

Siffatta impostazione appare giustificata dalle statistiche relative alla destinazione degli attacchi informatici, che segnalano come il 41% di questi sia stato diretto contro Pubbliche Amministrazioni[4], la maggior parte delle quali prive di un efficiente argine di *cybersicurezza* e troppo spesso lente nel segnalare le incursioni virtuali.

Ebbene, sulla falsariga del modello introdotto con il Codice in materia di protezione dei dati personali, il DDL prevede già all'art.1 l'obbligo di segnalazione e notifica a carico della Pubblica Amministrazione in ordine agli incidenti "*aventi impatto su reti, sistemi informativi e servizi informatici di rispettiva pertinenza*" (e cioè a dirsi agli incidenti di cui alla disposizione dell'art. 1, comma 3-*bis*, D.L. n. 105/2019[5]).

Il medesimo articolo delinea inoltre, insieme alle modalità e ai tempi per adempiere alla suddetta imposizione, le sanzioni derivanti dall'inosservanza di siffatti obblighi. Segnatamente, a seguito di un primo inadempimento, la Pubblica Amministrazione riceverà una preliminare comunicazione da parte dell'ACN contenente l'avvertenza che la prosecuzione della mancata notifica comporterà l'irrogazione delle sanzioni previste al successivo comma 5 (una sanzione amministrativa pecuniaria con forbice edittale che varia da euro 25.000 ad euro 125.000). A seguito dell'avviso, l'Agenzia promuoverà delle ispezioni, nelle forme di vigilanza collaborativa, volte a sostenere l'amministrazione interessata nello sforzo di rafforzamento della propria postura di resilienza cibernetica. Nei casi di reiterata inosservanza si procederà invece con la sanzione pecuniaria di cui sopra.

[4] Il Sole24ore: https://ntplusentilocaliedilizia.ilsole24ore.com/art/enti-pubblici-alert-azioni-cybercriminali-le-commesse-pnrr-AF4eT1TC .
[5] D.L. 21 settembre 2019, n. 105 "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica*".

Gli obblighi richiamati non trovano tuttavia applicazione né nei confronti dei soggetti di cui alle lettere g) e i) dell'art. 3, comma 1, D.Lgs. n. 65/2018, ossia agli operatori di servizi essenziali ed ai fornitori di servizi digitali (cd. soggetti NIS); né verso i soggetti di cui all'articolo 1, commi 2, lett. a), e 2-*bis*, D.L. n. 105/2019 (c.d. soggetti "*inclusi nel perimetro di sicurezza nazionale cibernetica*" o, solo, soggetti Perimetro); né nei confronti degli 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; né verso gli organismi di informazione per la sicurezza di cui agli articoli 4, 6 e 7 Legge n. 3 agosto 2007, n. 124.

Manifesta perciò la volontà di assicurare un ruolo centrale all'ACN, a cui vengono infatti assicurati poteri sia ispettivi che sanzionatori secondo una tendenza che trova conferma nel successivo art. 2, che sancisce il carattere prescrittivo delle segnalazioni dell'ACN: che fanno scattare un vero e proprio obbligo per il destinatario di procedere effettivamente con interventi risolutivi.

L'ACN avrà così maggiori responsabilità nella prevenzione degli attacchi e dovrà fungere da punto di riferimento per il coordinamento tra l'attività amministrativa e l'autorità giudiziaria.

Il DDL prevede altresì una riforma strutturale per le Pubbliche Amministrazioni: il dovere cioè di individuare una struttura, anche tra quelle già esistenti, preposta alla specifica attività di cybersicurezza; nonché, il dovere di istituire all'interno della stessa la figura di "Referente per la cybersecurity" (soggetto deputato ad appunto svolgere, tra l'altro, la funzione di contatto unico dell'amministrazione con l'ACN).

È proprio il "Referente per la cybersecurity" che sarà chiamato a fungere da "cinghia di trasmissione" tra l'ente pubblico e l'ACN.

Sulla singola amministrazione graverà (insomma) l'ulteriore onere di "collaborazione" attiva nella lotta al *cybercrime,* come chiaramente testimonia la stessa introduzione di sanzioni per la mancata notifica di un attacco.

Sul piano più strettamente penalistico e processuale le modifiche si incentrano sulle singole fattispecie delittuose: innalzamento delle pene; ampliamento dei confini del dolo specifico; previsione di nuove aggravanti; divieto di bilanciamento delle attenuanti in casi particolari.

Segnatamente, al capo II del DDL (artt. 11-18) sono collocate le disposizioni per la prevenzione ed il contrasto dei reati informatici, nonché di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici.

In specifico, all'articolo 11, comma 1, lett. a), si ritrovano interventi in ordine alla cornice edittale ed alle circostanze (compresi nuovi divieti di bilanciamento con circostanze attenuanti) della fattispecie incriminatrice di cui all'art. 615-*ter* c.p., rubricato "*Accesso abusivo ad un sistema informatico o telematico*".

Il testo attualmente vigente prevede che: "*1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. 2. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un 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 della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) 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. 3. Qualora i fatti di cui ai commi primo e secondo riguardino 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, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. 4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio*".

Il testo dell'art. 615-*ter* c.p., così come novellato dal DDL, risulterebbe quindi il seguente: "*1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. 2. La pena è della reclusione* ***da due a dieci anni****: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un 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 della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa* ***minaccia o*** *violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento* ***ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare*** *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. 3. Qualora i fatti di cui ai commi primo e secondo riguardino 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, la pena è, rispettivamente, della reclusione* ***da tre a dieci anni e da quattro a dodici anni****.* ***Nei soli casi in cui concorrono anche le circostanze previste dal numero 3) del secondo comma, le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-quater non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultante dall'aumento conseguente alle predette circostanze aggravanti.*** *4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio*".

Dal confronto delle due versioni risultano così manifesti:

- il raddoppio dei limiti edittali per le aggravanti di cui al secondo comma;
- l'estensione della punibilità per l'ipotesi aggravata di cui al numero 2) anche ai casi di "minaccia" (e non soltanto di "violenza");
- l'ampliamento della circostanza aggravante di cui al n. 3) anche ai casi di "sottrazione" del sistema o "inaccessibilità" al titolare allo stesso;
- l'ulteriore forte inasprimento delle pene previste al terzo comma;
- l'introduzione del divieto di bilanciamento delle aggravanti di cui al n. 3), comma 2, con le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-*quater* c.p.

All'articolo 11, comma 1, lett. b) DDL sono poi riportate le modifiche che dovrebbero interessare l'articolo 615-*quater* c.p.: fattispecie che sanziona la "*detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*".

Il testo attuale dell'art. 615-*quater* c.p. prevede: "*1. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164. 2. La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) al quarto comma dell'articolo 617*-quater".

A seguito delle propugnate modifiche l'art. 615-*quater* c.p. diverrebbe: "*1. Chiunque, al fine di procurare a sé o ad altri un* ***vantaggio*** *o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.* ***2. La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1). 3. La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma, primo periodo***".

Nel disegno "riformatore", oltre alla sostituzione del "profitto" con la locuzione più estensiva di "vantaggio", anche con riferimento all'art. 615-*quater* c.p. si assiste pertanto ad un sostanziale aumento di pena per la fattispecie aggravata di cui alla comma 2 (la pena, rispetto alla versione vigente, si prevede debba essere addirittura raddoppiata) e alla creazione di una nuova aggravante per l'ipotesi in cui oggetto materiale del reato siano "*sistemi di 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*".

Ancora, nelle intenzioni del Governo l'articolo 615-*quinquies* c.p., ora concernente la fattispecie incriminatrice di "*detenzione, diffusione ed istallazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*" dovrebbe essere di fatto ricollocata tra i delitti di danneggiamento, e, precisamente, all'interno della fattispecie di cui all'art. 635-*quater*.1 c.p.; delitto per il quale è (allo stato) previsto l'aggravarsi della pena in due ipotesi: "*quando ricorre taluna delle circostanze di cui all'art. 615*-ter, *secondo comma, numero 1)*" (reclusione da due a sei anni); "*quanto il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615*-ter*, terzo comma, primo periodo*" (reclusione da tre a otto anni).

Analoga estensione risulta operata pure con riguardo 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*". Si prevede infatti l'aumento della pena da due a sei anni "*quando ricorre taluna delle circostanze di cui all'art. 615*-ter*, secondo comma, numero 1)*".

Negli interventi di modifica è quindi possibile individuare un chiaro filo conduttore: comminare pene (in senso lato) severe per le ipotesi criminose relative al *cybercrime*. L'innalzamento dei limiti edittali, l'ampliamento del novero e dell'estensione delle circostanze aggravanti, il divieto di bilanciamento tra aggravanti e attenuanti, caratterizza invero ciascuno degli interventi che interessa il catalogo codicistico dei c.d. "reati informatici".

Prova ne 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*" e che pure si caratterizza per un sensibile aumento della cornice edittale per la circostanza aggravante di cui al comma 4 (da quattro a dieci anni, in luogo dell'attuale da tre a otto anni); rimodulazione ed estensione delle ipotesi aggravate; introduzione del divieto di bilanciamento tra aggravanti e circostanze attenuanti.

La nuova disposizione assumerebbe dunque i seguenti tratti: "*1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni. 2. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. 3. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. 4. Tuttavia si procede d'ufficio e la pena è della reclusione* ***da quattro a dieci anni*** *se il fatto è commesso: 1)* ***in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615*-ter*, terzo comma, primo periodo****; 2)* ***in danno di un***

pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale *o da un incaricato di un 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 della qualità di operatore del sistema;* ***5. Le circostanze attenuanti diverse da quelle di cui agli articoli 89, 98 e 623-quater , concorrenti con l'aggravante di cui al quarto comma, numero 1), non possono essere ritenute equivalenti o prevalenti e le diminuzioni di pena si operano sulla quantità della stessa risultate dall'aumento conseguente alla predetta aggravante***".

Nondimeno, il DDL introduce anche nuove circostanze attenuanti. La nuova disposizione di cui all'articolo 623-*quater* c.p. prevede infatti

- 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 così 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.[6]);

- 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 ad un'efficace attività di individuazione dei possibili responsabili; secondo una forma di soluzione non certo inedita, ma già introdotta (talvolta con profitto) in altri ambiti del nostro sistema penale (ad esempio per i delitti contro la fede pubblica[7]);

[6] 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*".

[7] 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*".

- infine, al terzo comma, all'evidente fine di massimizzare l'applicazione delle nuove attenuanti di cui sopra, è altresì stabilito 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 pur richiamate al comma 4 dell'art. 69 c.p.[8]).

Il DDL non si limita tuttavia a prevedere aggravi di pena e nuove circostanze attenuanti, perché fissa anche l'introduzione di nuove speciali figure di reato al precipuo fine di contrastare condotte criminose perpetrate a mezzo di strumenti informatici, sempre più frequenti e lesive in una società sempre più digitalizzata.

Esempio concreto di siffatta inedita politica legislativa sia l'introduzione nel codice penale di speciali figure criminose (complesse), quali, appunto, 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 nell'ultimo capoverso dell'articolo precedente*".

In senso analogo, il DDL apporta poi modifiche (pressocché identiche tra loro) alle ipotesi di danneggiamento di cui alle disposizioni degli artt.635-*bis* c.p., 635-*quater* c.p., 635-*ter* c.p. e 635-*quinquies* c.p. Per ognuna di siffatte disposizioni è invero previsto un innalzamento delle soglie edittali, la riscrittura delle aggravanti in ossequio alle modifiche apportate alle fattispecie aggravate dell'art. 615-*ter* c.p. (di cui si è detto sopra).

Al contrario, solo in relazione all'art. 635-*ter* c.p. e all'art. 635-*quinques* c.p. è previsto il divieto di bilanciamento tra circostanze aggravanti e attenuanti (fatte salve le circostanze attenuanti di cui agli artt. 89, 98 e 639-*ter* c.p.).

In ultimo, va segnalata l'introduzione dell'art. 639-*ter* c.p., che prevede circostanze attenuanti speculari a quelle di cui al 623-*quater* c.p. (ossia, diminuzione di pena per tenuità del fatto e per la collaborazione *post delictum*).

[8] 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*".

Sul piano processuale il DDL vorrebbe ricondurre tutte le fattispecie di criminalità informatica entro la disciplina ritagliata per i c.d. reati di criminalità organizzata (artt. 51 e 407 c.p.p.), così da consentire l'utilizzo dei più penetranti strumenti di indagine ed accertamento ed ampliando la competenza ed il coordinamento delle Direzioni distrettuali antimafia: profilo che (se da un lato) risponde all'esigenza di agevolare le indagini dinanzi a reati che si consumano in uno spazio (territorialmente) indefinito e potenzialmente assai vasto accentua e consolida (dall'altro) un sistema basato su diversi e distinti "binari" processuali.

Le modifiche al codice di procedura sono introdotte dall'articolo 12 del DDL: *(i)* vengono ricompresi nel novero delle fattispecie sottoposte alla competenza dell'Ufficio di Procura distrettuale i delitti di cui gli articoli 635-*quater*.1 c.p. (detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema telematico) e 635-*quinquies* c.p. (danneggiamento di sistemi informatici o telematici di pubblico interesse), nonché il delitto di cui all'articolo 1, comma 11, del D.L. n. 105/ 2019[9]; *(ii)* viene aggiunto nel novero dell'articolo 407, comma 2, lettera a), c.p.p. un nuovo numero 7-*ter*, inteso 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*".

E siffatta ultima disposizione viene altresì ricompresa 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).

L'articolo 13 del DDL modifica invece tre disposizioni (art. 9, comma 2; art. 11, comma 2; art. 16 *nonies*, comma 1) del D.L. n. 15 gennaio 1991, n. 8, sotto la rubrica "*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*".

[9] La disposizione prevede che: "*Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni*".

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[10].

Per gli stessi reati di cui al comma 4-*bis*, l'articolo 11 D.L. n. 8/1991 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 D.L. n. 8/1991, 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. 14 del DDL in esame modifica inoltre l'art. 13 D.L. 13 maggio 1991, n. 152 "*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*". Segnatamente, 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.

L'articolo 15 del DDL in commento interviene nell'ambito della responsabilità amministrativa derivante da reato. In particolare, mediante la modifica dell'art. 24-*bis* D.Lgs. 8 giugno 2001, n. 231 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 sanzioni pecuniarie derivanti dalla commissione di tale illecito vengono innalzate da trecento a quattrocento quote. 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*".

[10] 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*".

L’articolo 17 del DDL è poi inteso 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 dei servizi di telecomunicazione: disposizione funzionale a consentire al pubblico ministero di ricevere tempestivamente la notizia di reato. In aggiunta, vengono dettati obblighi informativi nei confronti del Procuratore nazionale antimafia e antiterrorismo. Per converso, nell’ipotesi in cui sia il pubblico ministero a divenire edotto di una notizia dei delitti di cui all’art. 371-*bis*, comma 4-*bis*, c.p.p., viene a questi imposto di darne tempestiva informazione all’Agenzia e di assicurare il raccordo informativo con il Ministero dell’interno per la sicurezza e per la regolarità del servizio di telecomunicazione.

Nell’ambito di suddette modifiche l’art. 17 del DDL in commento impone (da ultimo) al pubblico ministero di impartire “*le disposizioni necessarie ad assicurare che gli accertamenti urgenti siano compiuti tenendo conto delle attività svolte dall’Agenzia, a fini di resilienza, di cui all’articolo 7, comma 1, lettere n) e n-bis)*”, disponendo altresì della facoltà di differire “*una o più delle predette attività, con provvedimento motivato adottato senza ritardo, per evitare un grave pregiudizio per il corso delle indagini*”.