CAMERA DEI DEPUTATI – AUDIZIONE INFORMALE IN REFERENTE, PRESSO LE COMMISSIONI RIUNITE I E II DELLA CAMERA DEI DEPUTATI, DEL DISEGNO DI LEGGE C. 1717 GOVERNO, RECANTE " DISPOSIZIONI IN MATERIA DI RAFFORZAMENTO DELLA CYBERSICUREZZA NAZIONALE E DI REATI INFORMATICI

SINTESI DEL CONTRIBUTO DEL PROF. GIUSEPPE CORASANITI

Ordinario di informatica giuridica Universitas Mercatorum e LUISS

Già Sostituto Procuratore generale della corte di cassazione

(https://orcid.org/0000-0002-4905-3141)

Corasaniti-curriculum-completo--2023.pdf (unimercatorum.it)

Si esprime un **parere generalmente molto positivo** sulle disposizione del DDL in esame , in particolare sul potenziamento delle funzioni della Agenzia per la cybersicurezza nazionale e sull'affidamento di funzioni di valorizzazione dell'intelligenza artificiale come risorsa strategica , anche nel contrasto alla criminalità informatica con l'introduzione dell'art. 7 del DDL .

Pur tuttavia si intende suggerire alcune possibili integrazioni proprio nell'ottica di una migliore funzionalità del DDL attesa la rilevanza strategica del tema per il Paese e l'esigenza che sia affrontato alla luce dell'esperienza concreta del contrasto al cybercrime . In particolare si tratta di rafforzare significativamente il ruolo della Agenzia per la cybersicurezza nazionale e della stessa DNA ampliandone significativamente le competenze in tema di indagine su (tutti) i reati

informatici , che oggi coinvolgono organizzazioni criminali transnazionali . Si chiede di intervenite sulle problematiche della competenza in tema di reati informatici e rafforzando ulteriormente le disposizioni sanzionatorie in tema di frodi informatiche e trattamento illecito e fraudolento di dati personali in forma massiva.

1. Competenza territoriale dei pubblici ministeri in tema di reati informatici

Preliminarmente si ritiene importante suggerire - a seguito dei ripetuti contrasti territoriali tra pubblici ministeri in ordine alla competenza territoriale in materia di reati informatici - una possibile modifica **all'art. 8 del cpp** con determinazione della competenza del giudice distrettuale del **luogo dove si trova il sistema informatico e in caso di più sistemi con riferimento all'art. 9 comma 3 del cpp** , tale disposizione individuerebbe un momento di chiarezza e si rivelerebbe utilissima tanto più nel contesto attuale nel quale il disegno di legge governativo introduce una specifica competenza dell'agenzia nazionale per la cyber sicurezza e della direzione nazionale antimafia ed antiterrorismo.

Tale modifica sembra opportuna nel contesto del DDL in quanto esso introduce un coordinamento che finora è mancato tra attività di intervento immediato sul sistema compromesso e autorità giudiziaria nella specie requirente che tuttavia non è semplice individuare immediatamente anche per una costante incertezza giurisprudenziale persino a livello di Corte di Cassazione sui criteri che debbano prevalere nel caso di accertamento di reati informatici.

Ciò che spesso prevale è una rapidità delle forze di polizia negli accertamenti urgenti qui non sempre consegue una speculare rapidità nella conduzione delle indagini, le quali spesso debbono prevedere

acquisizione dei dati di *log* sui sistemi attaccati attraverso l'intervento del pubblico ministero in via d'urgenza. Sicché appaiono decisive le primissime ore al fine di acquisire immediatamente le tracce sui sistemi compromessi tenendo conto anche che spesso si tratta di attività per le quali viene richiesta una immediata attenzione da parte degli organismi requirenti se si vuole ottenere un risultato utile nelle indagini. Ne consegue che una precisa determinazione inequivoca della competenza territoriale che può delinearsi attraverso l'aggiunta di un comma all'articolo 8 del codice di procedura penale nel caso di accertamenti in materia di reati informatici risulterebbe fondamentale.

Peraltro tale specificazione legislativa appare del tutto coerente con la legge 24 luglio 2008, n. 125 (in G.U. 25/07/2008, n.173) che ha fissato appunto la competenza distrettuale anche del giudice in relazione alle indagini preliminari ed alla udienza preliminare , ma non è intervenuta sui criteri di determinazione della competenza rispetto ai reati informatici . Di qui l'utilità di un intervento di chiarificazione e semplificazione normativa per rendere più celeri ed efficaci in termini di resilienza gli interventi di accertamento immediati su sistemi informatici e dati .

2. Rafforzamento delle competenze distrettuali e nazionali sul cybercrime per DNA e DDA

Altrettanto si ritiene utile delinearsi con una **modifica contestuale dell'articolo 51 c. 3 quinquies cpp** che riguarda la competenza distrettuale dei pubblici ministeri in materia di reati informatici con l'inserimento delle nuove fattispecie di reato informatico tra cui quella prevista nel ddl di estorsione informatica (art. 629 CP) che non appare inclusa (limitando l'art. 12 del DDL integrazione solo alle ipotesi di cui

all'art. 635 quater e quinquies riformate dal DDL) ma anche degli articoli :

- **493 ter del codice penale**
- **493 quater del codice penale**

(ipotesi di reato introdotte dal Decreto legislativo 8 novembre 2021, n. 184 riguardanti la clonazione di carte di credito e strumenti di pagamento digitale e il possesso di strumenti e programmi per tale utilizzazione)

167

167 bis

167 ter

del Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (trattamento illecito di dati personali) trattandosi di comunicazione e diffusione fraudolenta e acquisizione fraudolenta ***almeno con riguardo all'uso illecito di dati personali su larga scala , tipica dei reati informatici su commissione*** (cybercrime by service) . Per tali ultime ipotesi di reato andrebbe anche valutato un significativo aumento del minimo e del massimo delle pene.

Si rileva l'opportunità di elevazione delle soglie di pena del reato di cui all'art. **640 quìnquies del Codice penale** frode informatica del soggetto esercente certificazioni telematiche , adeguando le relative pene attualmente minime incapaci di produrre una rilevante possibilità di indagine per tali ipotesi di reato (reclusione fino a tre anni) .

Tale indicazione riporterebbe coerenza e completezza al sistema normativo , poiché non tutti i reati informatici sono ricompresi nella competenza distrettuale e nel coordinamento della DNA , ed è invece molto opportuna una azione di intervento integrativo.

Analogamente sembra opportuna **una integrazione nella prevista integrazione dell'art. 407 comma 2 lettera a) con l'introduzione del nuovo comma 7 ter proprio in base al DDL in discussione .**

3. Problemi di coordinamento e di coerenza con il DDL nell'ottica di un rafforzamento complessivo delle strutture investigative e di governance

Si segnala l'opportunità di assegnazione di un ***più forte ruolo di coordinamento sul cybercrime alla Procura nazionale antimafia*** e antiterrorismo, anche per tali ipotesi di reato integrando tra i suoi compiti anche il contrasto alla criminalità informatica modificando in tal senso art 371 bis c. 4 bis del codice di procedura penale. Che già era stato oggetto di modifica nel 2015 , anche tale ruolo ,unito a quello della Agenzia impedirebbe l'insorgere di contrasti tra pubblici ministeri su tutte le indagini riguardanti reati informatici , andrebbe valutata inoltre l'opportunità di integrare la denominazione aggiungendo anche dopo terrorismo "e cybercrime" oppure " e criminalità informatica" . Tale denominazione sarebbe essenziale per il coordinamento anche a livello Europol delle relative attività e renderebbe più manifesto tale ruolo, che poi proprio il DDL opportunamente rafforza anche nel quadro della cooperazione internazionale.

In linea di massima potrebbe essere utile la **previsione di un sito web di informazione a cura della Agenzia per la Cybersicurezza** o dalla Polizia delle comunicazioni molto simile a quello presente negli Stati Uniti (https://www.fbi.gov/investigate/cyber) da parte delle omologhe agenzie con la pubblicazione costante delle statistiche riguardanti i reati informatici più diffusi e un prontuario di questioni e buone prassi rivolte a piccole e medie imprese . Sarebbe utile nell'ambito delle funzioni di coordinamento e potenziamento della medesima

Agenzia anche prevedere e rafforzare il coordinamento tecnico con Università e istituti di ricerca , anche per la stesura di codici di condotta e servizi di informazione immediata per gli utenti dei servizi compromessi e per le vittime di reato informatico. Esiste un problema di informazione preventiva , anche sul piano tecnico ma esiste anche un problema di coordinamento rapido delle forze di Polizia . L'ideale potrebbe essere la previsione di un Centro di coordinamento funzionale sul cybercrime interforze che consenta di includere la specializzazione strutturale della Polizia di Stato con particolare riguardo alla Polizia postale e delle comunicazioni ampliando al potenziamento e allo scambio di informazioni in materia di contrasto al crimine informatico di carattere ed economico e fraudolento (Guardia di Finanza) e territoriale (Carabinieri) .

Molto utile si valuta il profilo di **rafforzamento strutturale** che il DDL introduce in tema di funzioni dell'Agenzia per la cybersicurezza nazionale chiamata a operare immediatamente nei casi di più gravi attacchi informatici , ma non va sottovalutato anche il tema del suo ulteriore potenziamento anche in sede consultiva, consentendone una più agile forma di consultazione e di supporto al sistema pubblico e privato. Si pone anche il problema di assicurare sempre un diretto coordinamento con la convenzione sul cybercrime del 2001 in particolare cooperazione estera gruppi di intervento e informazione 24/24 in ottica interforze e ACN.

Si delinea perciò , proprio in base alle disposizioni del DDL , la **possibilità di modifica dell'art. 13 della legge 18 marzo 2008, n. *48*** *(Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento int*erno) con un intervento sull'art. 13 affidando esclusivamente al Ministero dell'interno il compito di designazione del punto di contatto 24/24 sulla cooperazione immediata in materia di cybercrime , peraltro proprio in base alle disposizioni oggi

in discussione tale compito potrebbe essere svolto mediante una cooperazione con ACN e DNA.

Tale disposizione si riferisce infatti a due funzioni essenziali in tema di cooperazione investigativa sul cybercrime che però andrebbero formalmente distinte in relazione a due distinte disposizioni della Convenzione del 2001 poiché l'art. 24 c 7 che attiene a estradizione e cooperazione internazionale mentre l'art. 27 c 2 , come è avvenuto in tutti paesi firmatari , attiene alla rapida acquisizione di dati utili alle indagini ed al coordinamento proattivo tra le forze di polizia .

4. Trasparenza e diffusione di dati statistici omogenei in tema di Data breach e rafforzamento delle sanzioni penali in tema di trattamento illecito di dati personali su vasta scala .

Si sottolinea ,infine, l'importanza della pubblicazione degli esiti statistici della previsione normativa di cui al Dlvo 196/2003 art 167 c 4/5/6 che attiene ad una comunicazione tra uffici del Pubblico Ministero e Garante per la protezione di dati personali in tema di trattamenti illeciti dolosi e su vasta scala di dati personali . O si rivede , sopprimendolo, tale obbligo informativo o si rende invece molto più efficace tale disposizione nell'ambito di un circuito trasparente e coerente con il contenuto del DDL oggi in discussione prevedendo la pubblicazione dei dati statistici annuali sul sito del Garante per la protezione dei dati personali . In ogni caso dovrebbe essere posto il problema valutando i dati disponibili . Si suggerisce di affidare alla ACN anche tale funzione in coerenza con il suo fondamentale ruolo centrale di raccordo pubblico/privato e di intelligence strategica sul cybersicurezza .

Si suggerisce perciò , in coerenza col contenuto del DDL di intervenire con *l'aggravamento delle pene almeno anche sull'art. 167*

ter del Dlvo 196/2003 (acquisizione fraudolenta di dati personali su larga scala) .

ALLEGATO CON DISPOSIZIONI DI LEGGE RICHIAMATE

Art. 2 **codice di procedura penale**

1-quater. Quando si tratta di procedimenti per i delitti indicati nell'articolo 51, comma 3-quinquies, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare sono esercitate, salve specifiche disposizioni di legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente" (comma introdotto con legge 24 luglio 2008, n. 125 (in G.U. 25/07/2008, n.173)

Art. 8 Codice procedura penale

Regole generali

1. La competenza per territorio è determinata dal luogo in cui il reato è stato consumato.

2. Se si tratta di fatto dal quale è derivata la morte di una o più persone, è competente il giudice del luogo in cui è avvenuta l'azione o l'omissione.

3. Se si tratta di reato permanente, è competente il giudice del luogo in cui ha avuto inizio la consumazione, anche se dal fatto è derivata la morte di una o più persone.

4. Se si tratta di delitto tentato, è competente il giudice del luogo in cui è stato compiuto l'ultimo atto diretto a commettere il delitto.

Art. 9 Codice procedura penale

Regole suppletive

1. Se la competenza non può essere determinata a norma dell'articolo 8, è competente il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione.

2. Se non è noto il luogo indicato nel comma 1, la competenza appartiene successivamente al giudice della residenza, della dimora o del domicilio dell'imputato.

3. Se nemmeno in tale modo è possibile determinare la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335.

Art. 51 Codice di procedura penale

Uffici del pubblico ministero - Attribuzioni del procuratore della Repubblica distrettuale

3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 414-bis, 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 609-undecies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente.

Art. 371 bis c.4-bis. Codice procedura penale

Il procuratore nazionale antimafia e antiterrorismo esercita le funzioni di impulso di cui al comma 2 anche in relazione ai procedimenti per i delitti di cui agli articoli 615-ter, terzo comma, 635-ter e 635-quinquies del codice penale nonché, quando i fatti sono commessi in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità, in relazione ai procedimenti per i delitti di cui agli articoli 617-quater, 617-quinquies e 617-sexies del codice penale. Si applicano altresì le disposizioni dei commi 3 e 4 del presente articolo

))

Art. 493-ter. codice penale ((Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti)).

Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ((o comunque ogni altro strumento di pagamento diverso dai contanti)) è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera ((gli strumenti o i documenti di cui al primo periodo)), ovvero possiede, cede o acquisisce ((tali strumenti)) o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.

In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre

utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.

Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.

Art. 167 Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali (Trattamento illecito di dati)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ((...)) arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

Art. 167-bis

(((Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala).))

((

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 167-ter (((Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).))

((

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 13.(Norma di adeguamento) Legge 18 marzo 2008, n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.)

1. L'autorità centrale ai sensi degli articoli 24, paragrafo 7, e 27, paragrafo 2, della Convenzione è il Ministro della giustizia.

2. Il Ministro dell'interno, di concerto con il Ministro della giustizia, individua il punto di contatto di cui all'articolo 35 della Convenzione.