Prof. Avv. Ranieri Razzante

Docente di Tecniche e regole della Cybersecurity
Università Suor Orsola Benincasa

Onorevoli Presidente e Deputati
Commissioni Riunite I e IX
Camera dei Deputati

Roma, 5 aprile 2025

Signori Presidenti, Onorevoli Deputati,

l'intento dell'intervento è chiaramente meritevole e risponde a un'esigenza fondamentale: rafforzare la protezione delle infrastrutture critiche nazionali da minacce informatiche in continua evoluzione.
La modifica proposta - l'introduzione della categoria di incidente ICP-A-20 relativa all'accesso non autorizzato o con abuso dei privilegi concessi - mira a colmare una lacuna significativa nell'attuale sistema di classificazione degli incidenti. Infatti, l'accesso non autorizzato o l'abuso di privilegi rappresentano vettori di attacco particolarmente insidiosi, spesso utilizzati nelle fasi iniziali di attacchi complessi e sofisticati. La relazione illustrativa chiarisce che l'obiettivo dell'intervento è "innalzare il livello di sicurezza nazionale nello spazio cibernetico, mediante la previsione di una fattispecie inclusiva di tutte le attività, anche non intenzionali, di accesso ai dati".
Questo approccio riflette una comprensione aggiornata delle dinamiche delle minacce cibernetiche contemporanee, riconoscendo che gli accessi non autorizzati o gli abusi di privilegi, anche quando non immediatamente dannosi, possono costituire precursori di attacchi più gravi o possono rivelare vulnerabilità sistemiche che necessitano di interventi preventivi.
Proprio in ossequio a quanto fin qui dedotto, appare opportuno soffermare l'analisi su alcune criticità che, in teoria, potrebbero frustrare l'obiettivo perseguito.

a) Criticità formali e procedurali

<u>Incongruenza nella data del DPCM oggetto di modifica</u>

La prima criticità che emerge dall'esame dello schema di DPCM riguarda un'incongruenza nella data del DPCM oggetto di modifica. Nel frontespizio e nel titolo dell'atto Camera si fa riferimento al "***decreto del Presidente del Consiglio dei ministri 13 aprile 2021, n. 81***", mentre il decreto effettivamente vigente e oggetto di modifica è datato "***14 aprile 2021, n. 81***".

Questa discrepanza potrebbe costituire un vizio di natura sostanziale in quanto potrebbe incidere in punto di certezza del diritto e sulla corretta collocazione delle modifiche nel sistema normativo vigente.

A corroborare tale tesi non ci si può esimere dal citare la *"Circolare della Presidenza del Consiglio dei Ministri del 2 maggio 2001, n. 1/1.1.26/10888/9.92*", recante "Guida alla redazione dei testi normativi", ove si raccomanda espressamente che i riferimenti ad altri atti normativi siano completi e precisi in tutti i loro elementi.

È significativo notare che questa incongruenza permane solo nel frontespizio e nel titolo, mentre nelle premesse e nell'articolato dell'atto la data viene correttamente indicata come "14 aprile 2021"; questa disomogeneità interna allo stesso atto normativo amplifica ulteriormente la criticità.

Come stabilito nella parte introduttiva della circolare, *"l'attenzione verso la qualità della regolazione si è andata accentuando in questi ultimi anni*" proprio perché *"la norma giuridica non è neutra, ma anzi orienta la dislocazione di risorse materiali ed umane*." Un'identificazione errata compromette la conoscibilità dell'atto da parte dei destinatari, vulnerando la funzione stessa della norma.

Sull'iter procedurale di adozione

Dalla documentazione trasmessa e come acutamente osservato dal Consiglio di Stato con il parere n. 00215/2025 – Dal quale non si intravede alcun motivo per discostarsi - vi sono alcuni elementi che meriterebbero un approfondimento.

Prendendo le mosse proprio dal citato parere emergono delle potenziali frizioni, nello specifico: l'articolo 1, comma 3, del decreto-legge n. 105/2019 stabilisce espressamente che il DPCM sia "adottato su proposta del CIC". Questa disposizione delinea un preciso procedimento di formazione dell'atto, che prevede la proposta formale da parte del CIC quale fase necessaria e imprescindibile dell'iter procedimentale.

Secondo detto Consesso, nella documentazione trasmessa non vi è traccia di tale proposta formale. Si rinviene invece una nota, datata 24 febbraio 2025, dell'Agenzia per la cybersicurezza nazionale e indirizzata al Dipartimento per gli Affari giuridici e legislativi, nella quale si fa riferimento a un "parere" del CIC. Tale nota, peraltro, è firmata dal Capo di gabinetto dell'Agenzia e non dal Direttore generale dell'Agenzia stessa, che ai sensi dell'articolo 4, comma 4, del decreto-legge n. 82/2021, "svolge le funzioni di segretario del Comitato".

Questa anomalia presenta delle criticità: sotto il profilo formale la nota è una comunicazione dell'ACN che fa riferimento a un "parere" del CIC.

La differenza non è meramente terminologica; infatti, **una "proposta" implica un atto di impulso e di iniziativa, con contenuti articolati e motivazioni; un "parere" è invece un atto consultivo che esprime una valutazione su un'iniziativa altrui. La norma citata richiede espressamente una "proposta" del CIC e non un "parere".**

Sotto il profilo sostanziale, la nota è firmata dal Capo di Gabinetto dell'ACN, mentre il decreto-legge n. 82/2021, all'articolo 4, comma 4, stabilisce che il Direttore Generale dell'ACN "*svolge le funzioni di segretario del Comitato*". Appare evidente, pertanto, che il Direttore Generale, in qualità di segretario del CIC, sia l'unico soggetto legittimato a esprimere formalmente la volontà del Comitato, garantendone l'imputabilità all'organo collegiale. Il Consiglio di Stato, nel suo parere, ha correttamente evidenziato quindi che questa irregolarità procedurale rischia di collocare la proposta al di fuori del corretto rapporto di imputazione organica, al CIC, della 'volontà' espressa da quest'ultimo. In altre parole, viene meno la certezza che la stessa volontà espressa nella nota sia effettivamente riconducibile all'organo collegiale competente, con possibili conseguenze sulla legittimità dell'intero procedimento.

Questa osservazione tocca un principio fondamentale del diritto amministrativo: l'imputazione organica, ovvero l'attribuzione degli atti compiuti da persone fisiche alla persona giuridica (in questo caso, l'organo collegiale CIC). Affinché l'imputazione sia valida, è necessario che l'atto sia compiuto dal soggetto legittimato secondo la legge.

In questo caso, **la sottoscrizione da parte del Capo di Gabinetto invece che del Direttore Generale crea un'incertezza sulla corretta imputazione della volontà al CIC medesimo, potendo configurare un vizio di legittimità dell'iter procedimentale.**

Va inoltre evidenziato, sempre riprendendo il parere n. 00215/2025, che la nota si limita a comunicare che il CIC "ha deliberato favorevolmente all'unanimità, in via preliminare, sulla proposta di adozione del decreto in parola", senza fornire alcuna indicazione sul contenuto effettivo della proposta né sulle motivazioni che hanno portato alla sua formulazione.

Queste carenze contenutistiche, se non documentalmente colmate, non consentono (nemmeno allo scrivente) di verificare la corrispondenza tra la proposta del CIC e lo schema di DPCM effettivamente trasmesso alle Camere.

Tale iter -*rebus sic stantibus*- potrebbe prestare il fianco a censure in punto di validità del conseguente atto.

Carenze nella documentazione di supporto

Un'ulteriore criticità procedurale di notevole rilevanza riguarda le carenze nella documentazione di supporto allo schema di DPCM, per come (anche qui) dedotto dal Consiglio di Stato.

In primo luogo, lo schema è stato esentato dall'Analisi di Impatto della Regolamentazione (AIR), come risulta dalla dichiarazione del Capo del Dipartimento per gli Affari Giuridici e Legislativi. Tale esenzione è stata motivata con il riferimento all'articolo 6, comma 1, lettera c), del DPCM 15 settembre 2017, n. 169, che consente l'esclusione dall'AIR per gli atti "riconducibili per omogeneità generale di materia e analogia di intervento" a determinate categorie.

Tuttavia, considerata la rilevanza della materia della cybersicurezza e l'impatto potenzialmente significativo della nuova categoria di incidente introdotta sulla gestione della sicurezza informatica dei soggetti inclusi nel perimetro, l'esenzione dall'AIR appare difficilmente giustificabile. L'AIR avrebbe infatti consentito di valutare più approfonditamente l'impatto della modifica su tutti i soggetti coinvolti e di esplorare eventuali opzioni alternative.

In secondo luogo, l'Analisi Tecnico-Normativa (ATN) allegata allo schema presenta significative lacune informative. In particolare, nella sezione dedicata alla verifica dell'utilizzo di dati e riferimenti statistici, l'ATN si limita a dichiarare genericamente che "Per la predisposizione del presente decreto sono stati utilizzati, nei diversi settori di intervento, dati e riferimenti statistici già disponibili presso Amministrazioni ed enti pubblici. Si tratta, in particolare, dei dati acquisiti nel corso dell'esperienza applicativa del D.L. Perimetro e del DPCM n. 81 del 2021".

Questa dichiarazione risulta estremamente generica e non consente di comprendere:

- quali specifici dati statistici siano stati considerati;
- quali amministrazioni ed enti pubblici li abbiano forniti;
- in che modo questi dati giustifichino l'introduzione della nuova categoria di incidente;
- quale sia stata l'incidenza degli eventi riconducibili alla nuova fattispecie nell'esperienza applicativa precedente.

L'assenza di questi elementi informativi non consente una valutazione adeguata delle motivazioni sottese alla modifica normativa e della sua proporzionalità rispetto alle esigenze di tutela della sicurezza cibernetica. Il Consiglio di Stato, nel suo ripetuto parere, ha evidenziato bene questa lacuna, sottolineando che dall'ATN "non emergono ulteriori elementi conoscitivi, in merito al tenore della proposta del CIC".

In definitiva, l'eventuale carenza documentale non si configura come mera imperfezione formale, ma come **potenziale *vulnus* alla trasparenza e in punto di motivazione dell'intervento normativo, il che potrebbe pregiudicare non solo la qualità della normazione, ma anche la sua efficacia applicativa.**

b) Il problema dell'indeterminatezza normativa

La nuova categoria di incidente ICP-A-20 viene descritta come "*Accesso non autorizzato o con abuso dei privilegi concessi. Il soggetto ha evidenza, anche sulla base di parametri quali-quantitativi, dell'accesso non autorizzato o con abuso dei privilegi concessi, dall'interno della rete, a dati digitali*".
L'indeterminatezza di questa formulazione si manifesta principalmente nel riferimento a "*parametri quali-quantitativi*" non definiti. Questo termine tecnico, in assenza di ulteriori specificazioni, presenta – a mio avviso - diverse problematiche:

1. **vaghezza semantica**: l'espressione "*parametri quali-quantitativi*" è intrinsecamente vaga. Il termine "quali-quantitativi" suggerirebbe una combinazione di elementi qualitativi (relativi alla natura o alle caratteristiche) e quantitativi (misurabili numericamente), ma senza ulteriori specificazioni risulta praticamente impossibile determinare quali parametri debbano essere considerati.
2. **assenza di soglie o criteri oggettivi**: non vengono fornite soglie, scale o criteri oggettivi per valutare quando un accesso non autorizzato o un abuso di privilegi raggiunga un livello tale da richiedere la notifica. Ad esempio, non si specifica se sia rilevante il volume di dati consultati, la durata dell'accesso non autorizzato, il numero di sistemi coinvolti, o altri parametri oggettivamente misurabili.
3. **mancanza di indicatori di gravità**: non viene indicato alcun livello minimo di gravità o impatto che l'incidente deve avere per far scattare l'obbligo di notifica, a differenza di quanto avviene in altre normative sulla sicurezza informatica (come il GDPR o la direttiva NIS).

Tale *vulnus* è ancor più evidente se si raffrontano i principali standard di riferimento del settore, che potrebbero fornire un valido supporto per una formulazione più precisa e "tassativizzante" della nuova categoria di incidente.
Ad esempio, la famiglia degli standard ISO/IEC 27000 rappresenta un riferimento fondamentale per la gestione della sicurezza delle informazioni a livello mondiale, con aggiornamenti regolari che riflettono l'evoluzione delle minacce e delle best practice.
Lo standard ISO/IEC 27035, dedicato specificamente alla gestione degli incidenti di sicurezza delle informazioni, adotta un approccio sistemico, integrando la classificazione degli incidenti all'interno di un processo più ampio di gestione della sicurezza.
La rilevanza di ISO/IEC 27035:2023[1] per la categoria ICP-A-20 risiede nella sua capacità di collegare la classificazione degli incidenti a processi operativi concreti. Lo standard definisce non solo cosa

[1] La norma ISO/IEC 27035:2023 "*Information security, cybersecurity and privacy protection — Information security incident management*" è lo standard internazionale che fornisce linee guida per la gestione degli incidenti di sicurezza delle informazioni. Questa versione, che aggiorna e sostituisce le precedenti, definisce un approccio strutturato in cinque fasi per la gestione degli incidenti:

costituisce un incidente rilevante, ma anche come tale incidente debba essere gestito nelle varie fasi, dalla rilevazione alla notifica, fino alla risposta.

In particolare, ISO 27035 introduce una metodologia di classificazione basata sull'analisi dell'impatto potenziale dell'incidente sui principi fondamentali della sicurezza delle informazioni: confidenzialità, integrità e disponibilità. Questo approccio permetterebbe di ancorare la valutazione degli accessi non autorizzati o degli abusi di privilegi a parametri oggettivi, come il livello di compromissione della confidenzialità dei dati o il grado di alterazione della loro integrità.

L'adozione dei criteri ISO aggiornati permetterebbe quindi di ancorare la valutazione degli accessi non autorizzati o degli abusi di privilegi a parametri oggettivi e riconosciuti a livello internazionale, armonizzando inoltre le procedure di notifica previste dal DPCM con i sistemi di gestione della sicurezza delle informazioni già implementati da molte organizzazioni in conformità a ISO/IEC 27001:2022.

Lo stesso dicasi per il framework del National Institute of Standards and Technology (NIST),[2] che offre un approccio strutturato ed oggettivo alla classificazione degli incidenti.

La sua adozione come modello per la definizione della categoria ICP-A-20 offrirebbe numerosi vantaggi in termini di chiarezza e determinatezza.

Il NIST Cybersecurity Framework affronta infatti il tema degli accessi non autorizzati con un approccio metodico e graduale. Gli incidenti non sono semplicemente classificati come "rilevanti" o "non rilevanti", ma vengono valutati lungo un continuum di gravità basato su parametri oggettivi e misurabili. Il NIST suggerisce di considerare la durata dell'accesso non autorizzato, il volume di dati potenzialmente compromessi, nonchèe il livello di privilegio ottenuto dall'attaccante.

Particolarmente utile è la categorizzazione NIST degli impatti degli incidenti in tre livelli (alto, medio, basso), ciascuno definito da criteri specifici. Un "impatto alto" potrebbe essere definito, ad esempio, come un accesso non autorizzato che persiste per più di 24 ore, coinvolge credenziali amministrative, o interessa dati classificati come critici. Tale approccio potrebbe facilmente sostituire

---

pianificazione e preparazione, rilevamento, valutazione, risposta e apprendimento. Lo standard include criteri specifici per la classificazione degli incidenti basati su impatto, gravità e altri parametri misurabili, con scale di valutazione chiaramente definite che consentono un'oggettiva categorizzazione. Particolarmente rilevante è la metodologia per valutare l'impatto sulla confidenzialità, integrità e disponibilità delle informazioni, che fornisce parametri quantificabili per determinare la gravità di un incidente. Cfr. https://www.iso.org/standard/78973.html

[2] La NIST Special Publication 800-61 Revision 3, "*Computer Security Incident Handling Guide*", pubblicata il 2 aprile 2024, rappresenta la versione più recente e attualmente in vigore della guida ufficiale del National Institute of Standards and Technology degli Stati Uniti per la gestione degli incidenti di sicurezza informatica. Questa revisione aggiorna la precedente Revision 2 del 2012 per affrontare l'evoluzione del panorama delle minacce informatiche e allinearsi con altri framework NIST più recenti. La guida mantiene l'impostazione di un framework completo con definizioni precise e metodologie di classificazione degli incidenti, ma aggiorna l'approccio per includere minacce contemporanee come ransomware, attacchi alla supply chain e minacce persistenti avanzate. I criteri oggettivi di classificazione basati su vettore di attacco, impatto funzionale, impatto informativo e tempo di ripristino sono stati rivisti e aggiornati, confermando la raccomandazione di stabilire soglie di gravità specifiche per determinare la necessità di notifica obbligatoria degli incidenti. Vedasi https://csrc.nist.gov/pubs/sp/800/61/r3/final

l'indeterminato riferimento a "parametri quali-quantitativi" con criteri specifici e comprensibili per gli operatori.

Ulteriormente non si dimentichi, ad esempio, il framework MITRE ATT&CK[3], che rappresenta un'evoluzione significativa nella comprensione e classificazione delle minacce informatiche. A differenza degli approcci più tradizionali, MITRE ATT&CK non si limita a classificare gli incidenti in base ai loro effetti, ma li contestualizza all'interno delle tattiche, tecniche e procedure (TTP) utilizzate dagli attaccanti.

Questo framework risulta particolarmente utile per definire con maggiore precisione tecnica la categoria ICP-A-20. MITRE ATT&CK cataloga in modo dettagliato le tecniche di accesso iniziale (TA0001) e di escalation dei privilegi (TA0004), fornendo una tassonomia completa e aggiornata delle modalità con cui gli attaccanti possono ottenere accessi non autorizzati o abusare dei privilegi concessi.

L'adozione di riferimenti a MITRE ATT&CK nella definizione della categoria ICP-A-20 consentirebbe di specificare con precisione quali tecniche di accesso non autorizzato debbano considerarsi rilevanti ai fini della notifica. Ad esempio, potrebbe essere specificato che sono soggetti a notifica gli accessi non autorizzati ottenuti mediante tecniche di credential access (come password spraying o brute force) o di privilege escalation (come l'abuso di vulnerabilità o l'hijacking di token di autenticazione).

Questo livello di dettaglio tecnico ridurrebbe significativamente l'ambiguità della categoria, fornendo agli operatori criteri concreti per identificare gli incidenti soggetti a notifica.

L' indeterminatezza non è solo un problema teorico, ma essa comporta implicazioni pratiche significative. **I soggetti inclusi nel perimetro di sicurezza nazionale cibernetica si potrebbero trovare nell'incertezza rispetto agli eventi da notificare, con il rischio di interpretazioni e applicazioni disomogenee. Il CSIRT Italia potrebbe ricevere notifiche di qualità e rilevanza variabili, complicando l'analisi comparativa e la risposta efficace. La mancanza di soglie di gravità potrebbe inoltre portare a un sovraccarico di segnalazioni di eventi minori, distogliendo risorse dalla gestione degli incidenti più significativi.**

[3] Il MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) Framework è una base di conoscenza globalmente riconosciuta che cataloga le tattiche, tecniche e procedure (TTP) utilizzate dagli aggressori nelle diverse fasi di un attacco informatico. Sviluppato dall'organizzazione no-profit MITRE, questo framework si basa su osservazioni reali di attacchi informatici e viene continuamente aggiornato. Il framework è organizzato in "tattiche" (categorie di obiettivi tecnici) e "tecniche" (metodi specifici per raggiungere tali obiettivi). Per ciascuna tecnica, il framework fornisce descrizioni dettagliate, esempi di utilizzo, metodi di rilevamento e contromisure. Particolarmente rilevanti per l'analisi sono le tattiche "Privilege Escalation" (TA0004), "Credential Access" (TA0006) e "Collection" (TA0009). Il framework fornisce indicatori molto specifici per identificare queste attività, che avrebbero potuto informare una definizione più precisa della nuova categoria di incidente. ICP-A-20. Vedi https://attack.mitre.org/tactics/TA0004/

Altra tematica da scandagliare riguarda la possibile sovrapposizione fra la nuova categoria ICP-A-20 e altre già esistenti nella tabella 1 dell'Allegato A.

La prima sovrapposizione significativa riguarda la categoria ICP-A-9, definita come "*Perdita e/o compromissione di credenziali utenti*". In molti scenari reali, l'accesso non autorizzato avviene proprio tramite l'uso di credenziali compromesse. Si consideri, ad esempio, il caso di un attaccante che ottiene le credenziali di un dipendente attraverso un attacco di phishing e le utilizza per accedere a dati riservati. Questo evento contiene elementi di entrambe le categorie: da un lato vi è stata una compromissione di credenziali (ICP-A-9), dall'altro vi è stato un accesso non autorizzato a dati digitali (ICP-A-20). In assenza di indicazioni chiare su quale classificazione debba prevalere, il soggetto notificante si trova di fronte a un dilemma interpretativo che potrebbe portare a classificazioni disomogenee o a doppia notifica per il medesimo incidente.

Analogamente, si evidenzia una potenziale sovrapposizione con la categoria ICP-A-16, descritta come "*Raccolta di credenziali (Credential Access)*. Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate". Si pensi al caso di un utente interno che acceda senza autorizzazione a un database contenente hash di password. Questo evento potrebbe essere classificato sia come raccolta di credenziali (ICP-A-16), in quanto finalizzato per l'appunto all'acquisizione di credenziali, sia come accesso non autorizzato a dati digitali (ICP-A-20), poichè vi è stato un accesso non autorizzato agli hash delle password. La sovrapposizione è particolarmente problematica quando l'accesso non autorizzato è propedeutico alla raccolta di credenziali, creando per tale via un'incertezza su quale aspetto dell'incidente debba essere considerato prevalente ai fini della classificazione.

Pertanto, ripeto, si rischia di avere classificazioni disomogenee, con soggetti diversi che classificano incidenti analoghi in modi differenti, compromettendo la comparabilità e l'analisi statistica degli incidenti *de quibus*. Inoltre, l'incertezza classificatoria potrebbe portare a una duplicazione di notifiche, con i soggetti che effettuano multiple segnalazioni per lo stesso incidente, classificandolo sotto diverse categorie e generando un sovraccarico informativo per il CSIRT Italia.

Un ulteriore aspetto problematico riguarda *l'incertezza sui tempi di notifica*. Sebbene la tabella 1 preveda in generale notifiche entro 6 ore, per alcune sottocategorie potrebbero esserci tempistiche specifiche diverse, creandosi incertezza su quando l'incidente debba essere segnalato. Infine, la sovrapposizione tra categorie rende difficile per il CSIRT Italia analizzare efficacemente le tendenze e l'evoluzione delle minacce, in quanto incidenti simili potrebbero essere classificati in categorie diverse, compromettendo la capacità di identificare pattern emergenti e adottare misure preventive adeguate.

Per risolvere queste criticità, sarebbe probabilmente opportuno (forse necessario) introdurre una chiara gerarchia tra le diverse categorie o indicare criteri di priorità per la classificazione. Ad esempio, si sarebbe potuto specificare che in caso di incidenti che presentano caratteristiche di più categorie, prevale quella relativa alla causa primaria dell'incidente o quella che rappresenta la fase più avanzata dell'attacco. In alternativa, si sarebbe potuto richiedere di indicare una classificazione primaria e classificazioni secondarie, per consentire una rappresentazione più completa e granulare dell'incidente. In assenza di tali indicazioni, la sovrapposizione tra la nuova categoria e quelle preesistenti rischia di creare – giova ripeterlo - confusione e disomogeneità nelle segnalazioni, compromettendo l'efficacia del sistema di notifica degli incidenti.

c) Problematica distinzione tra notifiche obbligatorie e volontarie

Il DPCM n. 81/2021 prevede un sistema di notifiche articolato su due livelli distinti ma complementari. Da un lato, l'articolo 3 disciplina le notifiche obbligatorie per gli incidenti classificati nelle tabelle 1 e 2 dell'Allegato A, che devono essere effettuate rispettivamente entro 6 ore e 1 ora dal momento in cui il soggetto ne viene a conoscenza. Dall'altro, l'articolo 4 prevede la possibilità di notifiche volontarie per incidenti che non rientrano nelle categorie delle tabelle 1 e 2, ma che i soggetti inclusi nel perimetro ritengono comunque opportuno segnalare al CSIRT Italia.

Questa distinzione non è meramente formale, ma risponde a una precisa logica operativa. L'articolo 4, comma 2, stabilisce infatti che "Le segnalazioni ricevute ai sensi del comma 1 sono trattate dal CSIRT Italia in subordine rispetto alle notifiche di cui all'articolo 3". Tale disposizione delinea una chiara gerarchia tra notifiche obbligatorie e volontarie, stabilendo una priorità di trattazione per le prime, che si presume riguardino incidenti di maggiore gravità o impatto sulla sicurezza nazionale.

In questo contesto e come precedentemente già sostenuto, la formulazione della nuova categoria ICP-A-20 solleva una criticità significativa: l'assenza di soglie minime di gravità o impatto per l'attivazione dell'obbligo di notifica. La categoria viene descritta come "*Accesso non autorizzato o con abuso dei privilegi concessi. Il soggetto ha evidenza, anche sulla base di parametri quali-quantitativi, dell'accesso non autorizzato o con abuso dei privilegi concessi, dall'interno della rete, a dati digitali*", senza specificare quando un tale accesso o abuso raggiunga un livello di significatività tale da richiedere una notifica obbligatoria.

Questa impostazione contrasta con l'approccio adottato in altre normative in materia di sicurezza informatica, che prevedono esplicitamente che l'obbligo di notifica scatti solo per incidenti con un impatto significativo.

A mero titolo esemplificativo, la Direttiva NIS 2 (Direttiva UE 2022/2555) introduce una distinzione tra incidenti significativi ed incidenti rilevanti. I primi sono eventi che hanno causato o sono in grado

di causare una perturbazione grave delle attività dei soggetti obbligati o dei servizi che forniscono, richiedendo una notifica completa con tempistiche progressive. I secondi sono eventi con impatto transfrontaliero significativo che interessano la fornitura di servizi a o da altri Stati membri dell'UE, soggetti a procedure di notifica specifiche che coinvolgono il punto di contatto unico e la rete di CSIRT europei. La direttiva stabilisce criteri oggettivi per questa classificazione, includendo il numero di utenti colpiti, la durata dell'incidente, l'estensione geografica, il grado di perturbazione del servizio e l'impatto economico e sociale, garantendo così un approccio proporzionato agli obblighi di segnalazione.

L'assenza di una soglia minima di gravità nella nuova categoria ICP-A-20 comporta che qualsiasi accesso non autorizzato o abuso di privilegi, indipendentemente dalla sua rilevanza o impatto, rientri nell'obbligo di notifica. Questo approccio non distingue tra scenari molto diversi: accessi non autorizzati isolati e di limitato impatto, accessi sistematici o estesi con potenziale compromissione di dati sensibili, abusi di privilegi occasionali senza conseguenze significative, o abusi di privilegi come parte di attacchi coordinati con impatto rilevante.

Le conseguenze possono essere significative.

I soggetti inclusi nel perimetro, per evitare sanzioni, potrebbero notificare come incidenti ICP-A-20 anche eventi di scarsa rilevanza che, in un sistema più strutturato, rientrerebbero nelle notifiche volontarie. Questo potrebbe portare a un sovraccarico del CSIRT Italia con segnalazioni di eventi minori, deviando risorse da incidenti più gravi e compromettendo la capacità di risposta tempestiva alle minacce più significative.

D'altra parte, l'obbligo di notifica entro 6 ore per qualsiasi accesso non autorizzato o abuso di privilegi, indipendentemente dal suo impatto, impone oneri potenzialmente sproporzionati ai soggetti inclusi nel perimetro. Questi si troverebbero a dover monitorare e segnalare anche eventi di limitata rilevanza, con un dispendio di risorse che potrebbe non essere giustificato dai benefici in termini di sicurezza nazionale.

È significativo notare che l'articolo 3, comma 1, del DPCM n. 81/2021, specifica che i soggetti inclusi nel perimetro notificano gli incidenti "aventi impatto" su un bene ICT. Questa formulazione suggerisce che debba esserci un impatto concreto e significativo sul bene ICT, non una mera potenzialità o un rischio astratto. Tuttavia, la mancata specificazione di criteri per valutare la significatività dell'impatto nella nuova categoria ICP-A-20 contrasta con questa impostazione generale.

Come rilevato dal Consiglio di Stato nel (più volte giustamente citato) parere n. 00215/2025, l'indeterminatezza della nuova categoria rischia di renderla "meno distinguibile da quelle ex art. 4 dello stesso Dpcm", compromettendo il sistema di prioritizzazione delle notifiche. Se la distinzione

tra notifiche obbligatorie e volontarie diventa sfumata, viene meno il principio fondamentale secondo cui le risorse del CSIRT Italia dovrebbero essere prioritariamente dedicate agli incidenti più significativi.

L'introduzione di una soglia minima di gravità, con criteri oggettivi per valutare quando un accesso non autorizzato o un abuso di privilegi abbia un impatto tale da richiedere una notifica obbligatoria, avrebbe garantito una distinzione più chiara tra notifiche obbligatorie e volontarie, in linea con l'impostazione generale del DPCM n. 81/2021 e con gli standard internazionali in materia.

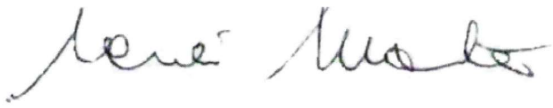
Tale approccio consentirebbe di concentrare le risorse sugli incidenti effettivamente significativi, migliorando l'efficacia complessiva del sistema di protezione della sicurezza cibernetica nazionale.

Potrebbe suggerirsi inoltre di **acquisire alla documentazione di supporto anche un quadro complessivo delle misure di sicurezza** e **delle procedure di monitoraggio** poste in essere dai soggetti inseriti nel perimetro di sicurezza nazionale cibernetica, che assumono rilievo in relazione alla fattispecie di nuova introduzione;

Tanto si propone a codesta Spettabile Autorità.

In fede

Prof. Avv. Ranieri Razzante



Via Guidubaldo del Monte, 13 – 00197 Roma Tel. 06-8417399
razzante@iusconsulting.it www.ranierirazzante.it