19 Settembre 2024

# Gli obblighi di gestione degli incidenti informatici per la crescita della fiducia nel digitale

*Di Giovanni Ferorelli*


## Abstract

La fiducia nel digitale va costruita con pazienza e lungimiranza, a partire dagli organi legislativi e governativi, e con il giusto e responsabile impegno di imprese e cittadini. Il processo passa anche, ma non solo, dalla costruzione di una normativa chiara sull'uso dei dati, sulla realizzazione di servizi digitali sicuri, in materia di cybersicurezza. A proposito di cybersicurezza: c'è un nuovo tassello che arricchisce ed integra il quadro normativo italiano di riferimento, ed è la Legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", che il presente elaborato mira ad analizzare.


## Indice



Le nostre vite, per come le conduciamo oggi, dipendono dai servizi digitali, fin dal principio della giornata, quando la sveglia impostata sullo smartphone ci ricorda che è il momento di alzarsi. Usufruiamo di beni e servizi, anche di primaria importanza, ci informiamo, intratteniamo relazioni e rapporti di lavoro grazie a Internet e al digitale e l'elenco potrebbe proseguire ancora per molto.

Se un servizio digitale è compromesso o addirittura smette improvvisamente di funzionare, o ancora, se è utilizzato in maniera subdola e all'insaputa degli utenti, a risentirne sono l'economia, la democrazia – si pensi, ad esempio, a quanto successo nel caso "Cambridge Analytica", o a tutti quei casi in cui l'accesso alle informazioni è pilotato da governi o da altri soggetti interessati – e più in generale il benessere e il progredire della società. Dunque, ognuno di noi, chi più chi meno.

> La fiducia nel digitale va costruita con pazienza e lungimiranza, a partire dagli organi legislativi e governativi, e con il giusto e responsabile impegno di imprese e cittadini. Il processo passa anche, ma non solo, dalla costruzione di una normativa chiara – e dal

> suo effettivo rispetto da parte dei relativi destinatari – sull'uso dei dati (personali e non), sulla realizzazione di servizi digitali sicuri e accessibili in maniera sicura, in materia di cybersicurezza. Altrettanto importante è l'attribuzione, all'interno di qualsiasi organizzazione, di ruoli e responsabilità chiari ed effettivi.

Il quadro normativo che si sta delineando, via via che i legislatori europeo e italiano pongono i vari tasselli, è un quadro complesso, che prevede adempimenti altrettanto complessi e il cui rispetto puntuale richiede **interazione tra diverse professionalità e competenze, sforzi importanti in termini di tempo, progettazione e risorse materiali e umane**. Queste ultime devono essere altamente qualificate e affidabili. Ciò è senz'altro vero nel contesto della protezione dei dati e della cybersicurezza, in cui devono coesistere competenze giuridiche, informatiche e tecniche, manageriali.

## Un nuovo tassello normativo

A proposito di cybersicurezza: c'è un nuovo tassello che arricchisce ed integra il quadro normativo italiano di riferimento, ed è la **Legge 28 giugno 2024, n. 90**, recante "**Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici**". Anche il rispetto degli obblighi previsti da tale legge può contribuire ad aumentare la fiducia nel digitale. Vediamo, quindi, come impatta sulle organizzazioni coinvolte.

La **Legge 28 giugno 2024, n. 90** introduce:

- al **Capo I**, disposizioni in materia di rafforzamento della cybersicurezza nazionale, di resilienza delle pubbliche amministrazioni e del settore finanziario, di personale e funzionamento dell'Agenzia per la cybersicurezza nazionale (di seguito "**ACN**") e degli organismi di informazione per la sicurezza nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici;
- al **Capo II**, disposizioni per la prevenzione e il contrasto dei reati informatici nonché in materia di coordinamento degli interventi in caso di attacchi a sistemi informatici o telematici e di sicurezza delle banche di dati in uso presso gli uffici giudiziari (non saranno, queste, oggetto del presente elaborato).

Si dà molta importanza alla gestione di incidenti aventi impatto su reti, sistemi informativi e servizi informatici. L'art. 1, in particolare, disciplina obblighi di segnalazione e notifica di tali incidenti. Vediamo più nel dettaglio di cosa si tratta.

## Gli Obblighi relativi alla gestione degli incidenti informatici

La norma in questione attribuisce ad alcune categorie di soggetti l'obbligo di segnalare e notificare ad ACN, secondo termini e modalità stabiliti, determinate tipologie di incidenti. Nei successivi paragrafi si indica chi è tenuto a procedere alla segnalazione, cosa in particolare deve essere segnalato, quando, e come.

## Chi

Destinatari dell'obbligo di segnalazione e notifica sono, fatte salve le eccezioni di cui al comma 7 dell'art. 1 della Legge 90/2024:

- le pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196, ossia le amministrazioni la cui ricognizione è operata annualmente dall'ISTAT;
- le regioni e le province autonome di Trento e di Bolzano;
- le città metropolitane;
- i comuni con popolazione superiore a 100.000 abitanti;
- i comuni capoluoghi di regione, anche se con popolazione pari o inferiore a 100.000 abitanti;

- le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- le aziende sanitarie locali, e
- le società in house dei soggetti sopra elencati e che forniscono servizi informatici e altri tipi di servizi.

Si precisa che, per espressa previsione legislativa, per alcuni dei sopra elencati soggetti gli obblighi di segnalazione e di notifica (meglio descritti al paragrafo successivo) decorrono dal 180° giorno successivo alla data di entrata in vigore della Legge 28 giugno 2024, n. 90.

## Cosa

L'obbligo consiste nel **segnalare** e nel **notificare** qualunque incidente avente impatto su reti, sistemi informativi e servizi informatici, che sia riconducibile ad una delle tipologie descritte nella **tassonomia degli incidenti** indicata con determinazioni tecniche del direttore generale, sentito il vice direttore generale, dell'**ACN**. Si veda, a tal proposito, l'Allegato A della Determina 3 gennaio 2023 dell'ACN, in cui è elencata una serie di tipologie di incidenti, raggruppati in diverse categorie: vi rientrano, a titolo esemplificativo, casi di accessi non autorizzati all'interno della rete, esecuzione non autorizzata di codice o malware all'interno della rete aziendale, comunicazioni non autorizzate verso l'esterno della rete. Sono, peraltro, i medesimi incidenti oggetto di notifica ai sensi dell'art. 1, comma 3-bis, del Decreto-legge 21 settembre 2019, n. 105.

Non a caso si è fatto separato riferimento alla segnalazione e alla notifica. Trattasi, a ben vedere, di due obblighi diversi: la notifica, successiva alla segnalazione, deve essere completa di tutti gli elementi informativi disponibili.

È fatta salva, in ogni caso, la possibilità di effettuare notifiche in forma volontaria aventi ad oggetto incidenti che non rientrano nella tassonomia di cui sopra. In tali casi – precisa il comma 4 dell'art. 1 della Legge 90/2024 – si applicherebbero le disposizioni dell'art. 18, commi 3, 4 e 5 del d. lgs. 18 maggio 2018, n. 65 (decreto legislativo che prevede un altro obbligo di segnalazione di determinati incidenti in capo ai fornitori di servizi digitali). E ciò, anche a tutela del segnalante, in quanto il citato comma 5 espressamente prevede che la notifica volontaria "non può avere l'effetto di imporre al soggetto notificante alcun obbligo a cui non sarebbe stato sottoposto se non avesse effettuato tale notifica".

## Entro quali termini

Sono individuati termini precisi da rispettare:

- la **segnalazione** deve essere fatta senza ritardo e comunque entro il termine massimo di **24 ore** ;
- la **notifica** entro **72 ore**.

Entrambi tali termini decorrono **dal momento in cui** i soggetti di cui al par. 1.1. **sono** "**venuti a conoscenza a seguito delle evidenze comunque ottenute**".

Sarà già venuto in mente, al lettore, un altro obbligo di notifica, e cioè l'obbligo di notifica di una violazione dei dati personali (**data breach**) all'autorità di controllo competente ai sensi dell'art. 33 del Regolamento (UE) 2016/679. Anche in tal caso, infatti, il termine entro il quale effettuare la notifica è di **72 ore** – la notifica oltre tale termine deve essere corredata dai motivi del ritardo – **decorrenti dal momento in cui il titolare del trattamento ne è venuto a conoscenza**.

Si noti che l'art. 1, comma 2, della Legge 28 giugno 2024, n. 90, introduce una precisazione in più rispetto all'art. 33 del GDPR, nella misura in cui fa riferimento alle "**evidenze comunque ottenute**" a seguito delle quali si verrebbe a conoscenza dell'incidente. Tale circostanza non sembrerebbe

introdurre una differenza rilevante nell'individuazione del momento da cui far decorrere i due termini di 72 ore. L'EDPB, infatti, nelle Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR, chiarisce il momento in cui il titolare del trattamento dovrebbe essere ritenuto essere venuto a conoscenza della violazione: "a controller should be regarded as having become "aware" when that controller has a **reasonable degree of certainty that a security incident has occurred** that has led to personal data being compromised." Ebbene, il ragionevole grado di certezza ben si concilia con le "evidenze **comunque** ottenute".

Le domande da farsi, piuttosto, sono: *quando, in un determinato contesto, il grado di certezza può ritenersi "ragionevole"?"* e *L'organizzazione dovrebbe fare qualcosa per trovarsi nella condizione di rilevare, e dunque venire a conoscenza, di un incidente informatico, oppure può limitarsi ad attendere che le evidenze in qualche modo si palesino?*

Anche a tali domande, per quanto riguarda la gestione dei data breach, le citate Linee guida offrono spunti interessanti, ma non è questa la sede per affrontarle. Ciò che qui preme evidenziare è che gli incidenti informatici ben possono rappresentare o causare violazioni di dati personali, pertanto la loro gestione va subito affrontata di raccordo con il DPO designato e con le altre funzioni pertinenti deputate alla gestione della politica di protezione dei dati personali.

## Come

Notifica e segnalazione devono essere effettuate tramite le apposite procedure disponibili nel sito internet istituzionale dell'ACN.

## Ulteriori elementi utili

I commi 5 e 6 prevedono un obbligo informativo dell'ACN in caso di inosservanza degli obblighi di notifica, e una sanzione amministrativa pecuniaria da 25.000 a 125.000 euro in caso di reiterazione dell'inosservanza, nell'arco di cinque anni, degli obblighi di notifica. Sempre a proposito di sanzioni, è espressamente previsto che la violazione degli obblighi di segnalazione e di notifica, "può costituire causa di responsabilità disciplinare e amministrativo-contabile per i funzionari e i dirigenti responsabili".

Inoltre, all'accertamento del ritardo o dell'omissione delle notifiche, possono seguire ispezioni da parte dell'ACN anche finalizzate a verificare l'attuazione, da parte dei soggetti interessati dall'incidente, di interventi di rafforzamento della resilienza agli stessi, direttamente indicati dall'ACN ovvero previsti da apposite linee guida adottate dalla medesima Agenzia.

## Ulteriori disposizioni

Di seguito si segnalano, senza pretesa di esaustività, alcuni aspetti contenuti in altre disposizioni del Capo I della Legge 90/2024 e che rilevano in particolar modo sulle organizzazioni in termini di compliance.

- **2**: l'ACN potrà segnalare specifiche **vulnerabilità** a cui determinati soggetti sono esposti, e a seguito della segnalazione tali soggetti avranno un termine entro il quale adottare gli **interventi risolutivi** indicati dalla stessa Agenzia, pena l'applicazione delle sanzioni richiamate al par. 1.5 e fatto salvo il caso in cui motivate esigenze di natura tecnico-organizzativa, da comunicare prontamente all'ACN, ne impediscano l'adozione o ne comportino un differimento oltre i termini previsti.
- **8**: è richiesto che i soggetti di cui al par. 1.1. – salvo eccezioni – individuino, nell'ambito delle loro risorse, una struttura a cui siano attribuiti diversi compiti e responsabilità impattanti in materia di sicurezza, e nell'ambito della quale sia individuato un **referente per la cybersicurezza**, il cui nominativo dovrà essere comunicato all'ACN in quanto tale soggetto fungerà da punto di contatto unico con l'Agenzia. Il comma 3 dell'articolo in questione chiarisce

che la struttura e il referente possano essere individuati, rispettivamente, nell'ufficio e nel responsabile per la transizione digitale previsti dall'art. 17 del d. lgs. 7 marzo 2005, n. 82.

- L' **9** introduce **obblighi specifici in materia di crittografia**, evidentemente ritenuta una misura fondamentale per garantire la sicurezza dei sistemi, se si considera anche quanto previsto dal successivo art.10 al quale si rimanda il lettore. Più precisamente è previsto l'obbligo, in capo a una serie di organizzazioni, di **verificare** "che i programmi e le applicazioni informatiche e di comunicazione elettronica in uso, che utilizzano soluzioni crittografiche, rispettino le **linee guida sulla crittografia** nonché quelle **sulla conservazione delle password** adottate dall'Agenzia per la cybersicurezza nazionale e dal Garante per la protezione dei dati personali e non comportino vulnerabilità note, atte a rendere disponibili e intellegibili a terzi i dati cifrati." Interessante notare il richiamo a tali linee guida.
- Sempre in tema di verifiche, l' **14** rinvia ad un separato decreto per l'individuazione, per specifiche categorie tecnologiche di beni e servizi informatici, di **elementi essenziali di cybersicurezza** che determinate categorie di soggetti dovranno tenere in considerazione nelle attività di approvvigionamento di beni e servizi informatici impiegati in specifici contesti.

## Conclusioni

Ebbene, dalla lettura della norma emerge chiaramente come la sua attuazione richieda ai relativi destinatari sforzi tesi a mettere in piedi una struttura e delle procedure funzionanti, un assetto organizzativo interdisciplinare, proattivo e animato da figure capaci di lavorare in sintonia, come se fossero parte di un unico corpo di ballo.

Anche da ciò dipenderà il grado di fiducia che i cittadini riporranno nel digitale.