Cloud PA. Più sicurezza con la qualificazione di ACN, ma sempre esposti al Cloud Act

Dal 19 gennaio prossimo ci sarà un'importante novità sulla qualificazione dei fornitori cloud per le Pubbliche amministrazioni. "Il bollino" non sarà più rilasciato da **AgID** ma dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Ecco perché i dati e i servizi delle nostre PA saranno più al sicuro con la qualificazione dell'Agenzia per la Cybersicurezza Nazionale

L'ACN potrà:

- successivamente al rilascio delle qualificazioni, effettuare verifiche per accertare il possesso e il mantenimento dei requisiti, in relazione alla tipologia e al livello di qualificazione.

Nell'ambito delle verifiche, l'Agenzia cyber nazionale, guidata da **Roberto Baldoni**, può:

1. formulare quesiti e richiedere informazioni;
2. richiedere la produzione di documentazione, ulteriori integrazioni e chiarimenti;
3. svolgere accertamenti di carattere tecnico, anche mediante accesso all'infrastruttura fisica e logica del servizio cloud;
4. audire il soggetto richiedente.

Ad oggi come avviene la qualificazione in AgID

Ad oggi AgID per i SaaS chiede la Cloud Security Alliance, in pratica una autovalutazione, mentre le altre certificazioni richieste ai Cloud Service Provider sono la ISO 9001 e ISO 27001, ma non sono, in generale, obbligatorie.

L'Agenzia ha previsto un periodo transitorio fino al 31 luglio, per garantire la continuità dei servizi qualificati già in uso alle amministrazioni e assicurare, così, un graduale passaggio verso un nuovo sistema coerente con le misure della Strategia Nazionale di Cybersicurezza e le indicazioni della Strategia Cloud Italia. Il regime ordinario partirà il 1^ agosto assieme al nuovo regolamento ACN e alla procedura di qualificazione online.

> *Chi dal 1^ agosto non rispetterà i nuovi requisiti di ACN va in incontro alla sospensione o alla revoca della qualifica posseduta.*

Le PA che scelgono servizi cloud di società USA restano esposti al Cloud Act

Quindi, avremo più sicurezza con la qualificazione di ACN dei Cloud Service Provider per le Pubbliche amministrazioni. Ma le PA che continueranno a scegliere fornitori che usano servizi cloud di società statunitensi saranno sempre esposti al Cloud Act e alle altre leggi Usa che obbligano queste aziende, che operano in Italia, a cedere i dati dei clienti alle agenzie governative degli Stati Uniti.

Nel dettaglio, Negli Stati Uniti sono in vigore tre leggi, il **Cloud Act**, **FISA 702 e EO 12333**, che obbligano le aziende

statunitensi che operano all'estero a cedere i dati dei loro clienti ai servizi Usa.

Il Cloud Act (Clarifying Lawful Overseas Use of Data Act) ha riformato la precedente normativa per dare più poteri di accesso ai dati "*posseduti, gestiti o controllati*" da servizi di comunicazione elettronica soggetti all'ordinamento USA. È la normativa che ha posto per prima l'attenzione degli studiosi sul tema della raggiungibilità giuridica del dato. La novità è che consente a un giudice USA, in caso di indagini su un reato, di emettere un ordine di accesso a dati che ritiene rilevanti, anche se i dati sono di titolarità di cittadini stranieri. È da sapere però che l'ordine sarà automaticamente eseguito senza potersi opporre solo se il proprio Stato abbia stipulato appositi accordi con gli USA per la sua attuazione.

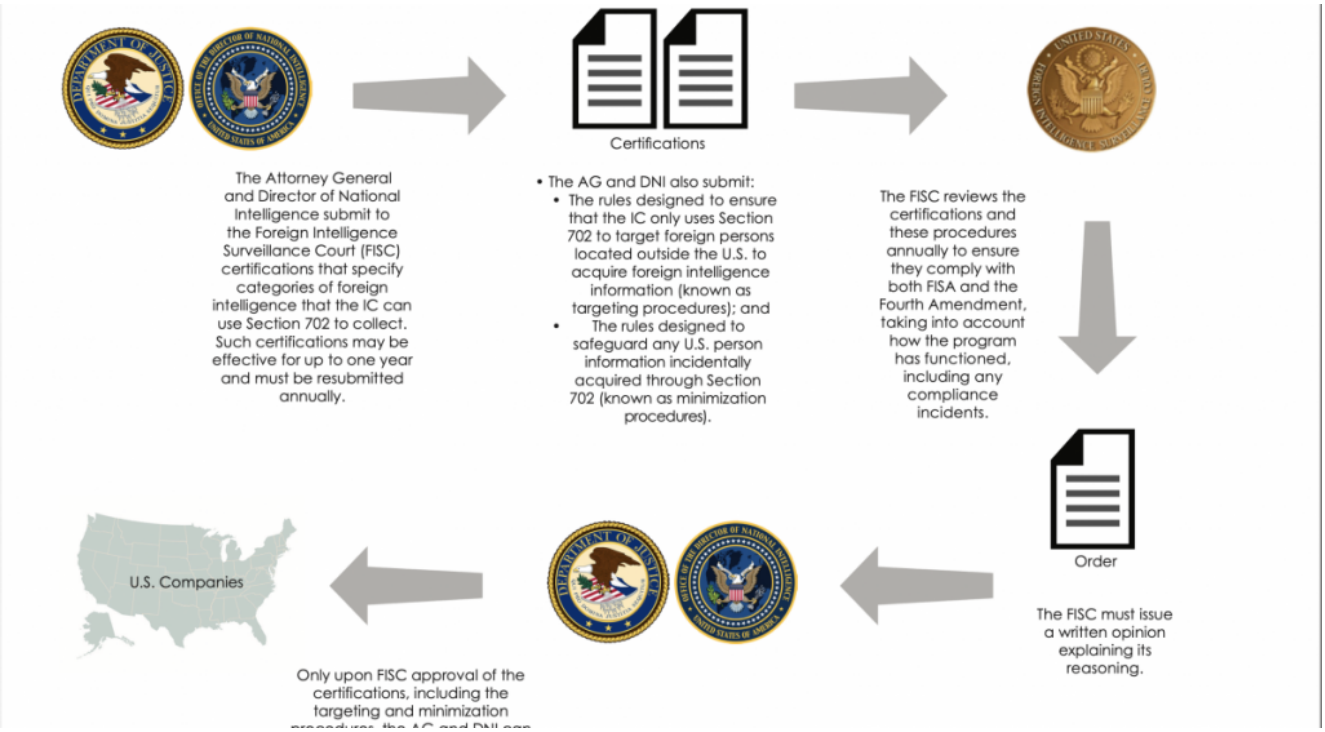
Invece EO 12333 è un "executive order". Praticamente, sottopone tutte le attività di intelligence, anche interne a quelle della CIA (esterne) e permette la raccolta indiscriminata di informazioni dai provider, sia riguardo ad americani sia a stranieri.

Ma maggior rischio per la sorveglianza di massa dei nostri dati è la **FISA** (Foreign Intelligence Surveillance Act), con la sua sezione 702.

È la legge antiterrorismo che autorizza la raccolta di qualsiasi comunicazione elettronica attraverso il computer o il telefono nei confronti di qualsiasi cittadino straniero fuori dagli Stati Uniti. Senza un mandato del giudice.

Parliamo di:

- nominativi di chi parla al telefono.
- il testo delle email.
- la cronologia di navigazione sul web con la motivazione dell'antiterrorismo.



La sorveglianza di massa consentita dalla FISA 702

Ai sensi della FISA 702, i *"fornitori di servizi di comunicazione elettronica"* statunitensi (come **Google, Amazon, Apple, Microsoft, Facebook, Google** e **Yahoo**), possono essere obbligati a concedere alle autorità di sicurezza statunitensi l'accesso ai dati personali di *"persone non statunitensi"*, definite come chiunque non sia cittadino statunitense o residente permanente negli Stati Uniti. Gli ordini di sorveglianza previsti da questa legge non devono essere specifici per un singolo obiettivo, ma consentono piuttosto un intero programma di sorveglianza a tappeto come **PRISM** o **Upstream**. Non esiste un'approvazione giudiziaria individualizzata per le persone non statunitensi. La FISA 702 consente anche la sorveglianza per scopi piuttosto ampi, come *"informazioni che … si riferiscono a … la condotta degli affari esteri degli Stati Uniti"*.

Allora come mitigare i rischi delle leggi USA?

L’obiettivo dell’ACN è agire su 2 fronti.

- *“La crittografia con due livelli, in base all’importanza dell’informazione che dobbiamo proteggere, con chiavi che verranno gestite in Italia”*, ha spiegato **Roberto Baldoni**, direttore generale dell’Agenzia, a settembre 2021 quando è stata presentata la Strategia Cloud Italia. *“Questo”,* ha aggiunto, “*riduce il rischio che un terzo soggetto possa vedere i dati in chiaro, non lo annulla completamente, perché ancora non abbiamo inventato una crittografia omomorfica computazionale, così c’è un processore nel mondo che vede quel dato”. “Però”,* ha assicurato, *“è molto più difficile per l’avversario sia fare incetta di dati sia effettuare l’estrazione del valore”.*

Infine, sul fronte della crittografia Baldoni ha anche annunciato *“l’algoritmo di crittografia nazionale*”. Ma non sarà una soluzione immediata*. “Ci darà delle garanzie in più, ma il suo sviluppo sarà graduale: non sarà un on-off”,* ha detto Baldoni, *“sarà pronta quando avremo un ecosistema in grado di gestirla, altrimenti può rivelarsi una vulnerabilità”.*

Nel frattempo, gli 007 statunitensi, se vogliono, hanno campo libero.

https://www.key4biz.it/cloud-pa-piu-sicurezza-con-la-qualificazione-di-acn-ma-sempre-esposti-al-cloud-act/429880/