Anac. Aidr: con lo Spid accesso veloce ad una serie di servizi

Dal 28 marzo è possibile accedere ad alcuni servizi online di Anac anche tramite Spid, il Sistema Pubblico di Identità Digitale. Con un unico nome utente e una sola password è, quindi, possibile fruire in modo veloce e sicuro di alcuni servizi digitali dall'Autorità Nazionale Anticorruzione già integrati con il nuovo sistema di autenticazione.

In particolare: il rilascio del Certificato esecuzione lavori (Cel) e le Attestazioni Soa (nuova versione). Il primo servizio è rivolto al Responsabile unico del procedimento (RUP) delle stazioni appaltanti che rilascia il Certificato all'impresa esecutrice di lavori pubblici che ne abbia fatto richiesta. Il secondo servizio invece è dedicato al rilascio delle attestazioni da parte delle Società Organismi di Attestazione (Soa).

"L'implementazione digitale da parte dell'Autorità Nazionale Anticorruzione – A.N.A.C, guidata da Giuseppe Busia – sottolinea in una nota Aidr – va in direzione di una sempre maggiore copertura di servizi digitali da parte della pubblica amministrazione con conseguente ottimizzazione dei tempi e delle relative procedure.

Nel 2021 lo Spid-. ricorda l'associazione Aidr in una nota – ha raggiunto il 43% della popolazione, con 26 milioni di identità rilasciate a fine ottobre dello scorso, più del doppio di quelle dello stesso periodo del 2020".

Direttiva NIS2: prendono forma le nuove norme europee sulla sicurezza informatica e delle reti

Il Consiglio Europeo ed il Parlamento europeo hanno recentemente raggiunto un'intesa politica sulle nuove misure per un livello comune elevato di cibersicurezza in tutta l'Unione, al fine di migliorare ulteriormente la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo insieme.

Si tratta della nuova Direttiva denominata "NIS2" che, una volta definitivamente adottata, andrà a sostituirà l'attuale Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (NIS), primo strutturato atto legislativo a livello europeo sulla sicurezza informatica, ancora in corso di vigenza.

Adottata nel lontano maggio 2016 la e recepita in Italia con il D.lgs. 18 maggio 2018, n. 65 (anche detto "decreto legislativo NIS"), la NIS ha risposto alla progressiva esposizione dell'Europa alle minacce informatiche che nel corso degli anni sono diventate sempre più frequenti e pervasive, per via di un aumento esponenziale della superficie esposta nell'ecosistema digitale, ormai sempre più eterogeneamente interconnesso.

La direttiva NIS2 mira a fronteggiare ulteriormente questo trend di escalation cyber, rispondendo all'esigenza di protezione, in modo omogeneo nel lungo termine, a livello europeo, dei servizi e presidi essenziali e strategici di ciascuno Stato membro, includendo adesso anche Organizzazioni di medie e grandi dimensioni di più settori critici per

l’economia e la società, compresi i fornitori di servizi pubblici di comunicazione elettronica, servizi digitali, acque reflue e gestione dei rifiuti, produzione di prodotti critici, servizi postali e di corriere e pubblica amministrazione, sia a livello centrale che regionale.
Il requisito dimensionale rappresenta peraltro una delle novità maggiormente significative dell’intesa politica perché i soggetti inclusi nell’alveo applicativo della nuova Direttiva verranno espressamente indicati dal Legislatore europeo, che ne circoscriverà l’ambito sulla base dei criteri di proporzionalità, un livello di gestione del rischio e criticità.
A tal riguardo vale la pena di evidenziare che la NIS2 si applicherà agli enti della pubblica amministrazione a livello centrale e regionale, riservandosi ai singoli Stati membri l’opportunità di estenderne l’applicazione a livello più periferico.

La NIS2 includerà anche l’adozione di misure di gestione del rischio di cibersicurezza per il settore sanitario, con particolare riferimento ai produttori di dispositivi medicali, proprio per rispondere alle crescenti minacce alla sicurezza rilevate durante la pandemia di COVID-19.
Dunque, la nuova direttiva intende rafforzare i requisiti di sicurezza informatica imposti alle aziende, attraverso l’introduzione di un quadro normativo che preveda un meccanismo più omogeneo ed efficace sia in termini di requisiti sia di misure di sicurezza, per la cooperazione nella gestione del rischio, degli incidenti nonché per lo snellimento degli obblighi di segnalazione in tutti i settori che rientrano nel perimetro dalla direttiva, nell’ambito di EU-CyCLONe, ossia dell’organizzata rete europea di collegamento per le crisi informatiche, che sosterrà la gestione coordinata degli incidenti di sicurezza informatica su larga scala e favorirà la condivisione di best practices a livello nazionale ed europeo.
A tal riguardo, la NIS2 nell’aggiornare l’elenco dei settori e

delle attività soggetti agli obblighi di sicurezza informatica andrà anche a prevedere una serie di rimedi e sanzioni per garantirne l'effettiva applicazione.

A tal proposito, di fondamentale importanza è il tema della sicurezza delle catene di approvvigionamento e delle relazioni con i fornitori che vede introdurre adesso la responsabilità del top management nel caso di mancata osservanza degli obblighi di sicurezza informatica, introducendo altresì misure di vigilanza più rigorose per le autorità nazionali.

L'accordo provvisorio raggiunto, nel caso di definitiva approvazione da parte del Consiglio europeo e del Parlamento europeo prevederà a carico degli Stati membri un generale obbligo di recepimento della nuova Direttiva negli ordinamenti giuridici nazionali nel termine dilatorio di 21 mesi dalla sua entrata in vigore.

Web Reputation, la difesa della propria identità online

C'è un termine, entrato negli ultimi anni prima nel vocabolario comune e poi, sulla **Treccani: googlare**. Il verbo in questione indica molto di più della mera azione di ricerca sul web, ma abbraccia un concetto più ampio, quello della conferma di una nostra iniziale percezione.

Per capirne realmente la forza e la portata innovativa basta guardare alle nostre azioni quotidiane: ho visto un prodotto, ho sentito alla radio il nome di una certa località, mi hanno parlato bene di un certo dentista, in tutte queste situazioni, l'azione che immediatamente segue il primo impulso (per usare un termine caro al marketing) è quella di cercare conferma

online e appunto googlare: il nome della località in questione, o del professionista sanitario, o del prodotto specifico, per tornare all'esempio sopracitato. Nel nostro viaggio online, alla ricerca di conferme e recensioni positive (i professionisti del marketing chiamerebbero questa fase **Zero Moment of Truth** (ZMOT) ci imbattiamo in una serie di informazioni, frutto di recensioni e giudizi altrui, lasciati nel grande spazio libero del web. Già lo spazio libero del web, un mondo senza vincoli e barriere che rischia di essere anche un mondo senza regole.

Cosa succederebbe infatti se, per tornare all'esempio di cui sopra, googlando sul web mi imbattessi in una serie di recensioni negative sul professionista sanitario di cui stavo cercando informazioni, quali effetti avrebbero sulla mia scelta, quali sulla reputazione del sanitario in questione?

Qui veniamo al nodo forse più spinoso della web reputation, che comprende non soltanto tutte le informazioni che forniamo noi in prima persona sul web o sui nostri account social: foto, video, pensieri condivisi in libertà, ma altresì ciò che gli altri più o meno consapevolmente, più o meno volontariamente scrivono su di noi. Foto pubblicate da altri, recensioni lasciate su portali dedicati, post pubblicati sul proprio account che fanno riferimento ad uno specifico prodotto, articoli scritti su blog.

Gli esempi sono tendenzialmente infiniti, così come le occasioni che il web offre per esprimersi. Cosa ha spinto quella persona a raccontare in termini negativi l'esperienza vissuta, quali erano le aspettative dell'acquirente sul prodotto? In realtà le variabili sono tantissime e spesso e volentieri, diventa difficile per l'avventore che legge un commento o una recensione sul web, riuscire a cogliere le mille sfumature che si celano dietro una frase e che sono sintetizzate in una recensione negativa, o in un Non mi piace, piuttosto che in una emoticon con l'espressione arrabbiata, o in un coinciso non lo consiglio. Ma chi controlla tutta questa

mole di informazioni, cosa possiamo fare realmente per tutelarci? Vero, il web è sì un mondo virtuale, ma non svincolato dalle leggi, quindi in teoria, possiamo far valere gli stessi principi e le stesse norme che disciplinano nel mondo reale il diritto all'immagine, alla reputazione, e parimenti la tutela dalla diffamazione. Purtroppo però, non sempre è così semplice. Ancor più tortuoso il diritto all'oblio, la sacrosanta richiesta di non essere marchiato a vita online, di veder cancellati dati e informazioni, non (più) corrispondenti alla nostra identità. Il monitoraggio costante, la costruzione della web reputation diventano così elementi imprescindibili per il privato cittadino e ancor più per le aziende.