

Interrogazione a risposta scritta

Visti

- il “Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” (c.d. “Regolamento generale sulla protezione dei dati” o “GDPR”), in particolare, l’art. 4, che definisce la “violazione dei dati personali” (c.d. “data breach”) come “la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati”, l’art. 33 che prevede l’obbligo di notifica dei data breach al Garante per la protezione dei dati personali, salvi i casi in cui sia “improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche”, l’art. 34 che prevede l’obbligo di comunicare, in alcuni casi, le violazioni di dati personali anche agli interessati, e gli artt. 37, 38 e 39 che definiscono, rispettivamente, la designazione, la posizione e i compiti del Responsabile della protezione dei dati;
- il D.Lgs. 30 giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali” e s.m.i.;
- la determinazione del 6 ottobre 2023, n. 20827, del Direttore Generale “Cura della persona, Salute e Welfare”, recante “Costituzione del tavolo regionale per il coordinamento delle misure in materia di protezione dei dati personali delle Aziende e degli Enti del SSR”, in particolare, laddove si prevede che **“la società Lepida S.c.p.A, è la società in house degli enti del SSR e della Regione, impegnata nella progettazione, ricerca, sviluppo, sperimentazione e gestione di servizi e prodotti ICT, con una linea di alta specializzazione nei settori della sanità, dell’assistenza sociale, dei servizi degli enti locali alla persona e del socio-sanitario”**;
- la deliberazione della Giunta regionale del 20 giugno 2022, n. 1004, recante “Definizione di competenze e responsabilità in materia di protezione dei dati personali. Abrogazione della deliberazione di Giunta regionale n. 1123/2018”, che individua il modello organizzativo privacy della Regione Emilia-Romagna;
- la determinazione n. 19293, del 4 novembre 2020, del Direttore generale “Risorse, Europa, Innovazione e Istituzioni” della Giunta regionale dell’Emilia-Romagna avente ad oggetto “Disciplinare tecnico per la gestione degli incidenti di sicurezza e data breach” e, in particolare, l’Allegato della stessa che stabilisce come per “incidente di sicurezza”, deve intendersi “l’evento o serie di eventi che hanno effettivamente impatto negativo sulla sicurezza o sulle performance dei sistemi come la violazione o la minaccia imminente di violazione di una policy di sicurezza informatica, di politiche di utilizzo accettabili o di prassi standard di sicurezza, correlato ad una violazione di dati o informazioni”, nonché, la deliberazione della Giunta regionale n. 1249, del 22 luglio 2019, recante “Approvazione della politica generale sulla sicurezza delle informazioni dell’Ente”;

premessato che

- il 28 novembre 2023 un attacco informatico, del tipo *ransomware*, ha colpito l’Azienda Usi di Modena, l’Azienda Ospedaliero-Universitaria di Modena e l’Ospedale di Sassuolo (MO)

paralizzando le attività dei centri prelievi, delle visite specialistiche e delle prestazioni ambulatoriali, con la conseguenza che le suddette strutture sanitarie sono state costrette a ritornare al “vecchio” cartaceo ed i cittadini a fare i conti con disservizi di varia natura e procedure più lente e complesse, fino a casi di mancata erogazione di servizi e prestazioni sanitarie;

- secondo alcuni siti specializzati l’attacco sarebbe stato rivendicato l’11 dicembre scorso da un gruppo di criminali informatici denominati *Hunter International* che opererebbe proprio con l’obiettivo di *esfiltrare* dati e ricattare le vittime richiedendo somme ingenti per il riscatto e il gruppo avrebbe dichiarato di aver sottratto 1.202.175 documenti, per un peso complessivo di 954 gigabytes, chiedendo tre milioni di dollari di riscatto in criptovalute;
- la stessa Azienda USL di Modena avrebbe comunicato che i suddetti criminali informatici avrebbero provveduto alla pubblicazione, nelle giornate del 13 e 14 dicembre scorso, nel *dark web*, cioè quella parte della Rete Internet non indicizzata e che può essere raggiunta solo da applicazioni particolari, di numerosi files contenenti dati aziendali anche di natura sanitaria e che dalle verifiche effettuate risulterebbe che i dati non sarebbero stati perduti irrimediabilmente dall’Azienda, ma copiati, circostanza che non diminuisce la gravità di quanto accaduto;

considerato che

- il GDPR, all’art. 37, comma 1, lett. c), rende obbligatoria per gli Enti del SSR la nomina del Responsabile della protezione dei dati (c.d. “*Data Protection Officer*” o “*DPO*”), individuando in tale figura il fulcro del processo di attuazione del principio di “*responsabilizzazione*” alla base della normativa europea in tale settore;
- ancora il 4 gennaio 2024, malgrado il lavoro dei tecnici delle Aziende sanitarie modenesi, non era ancora stato ultimato il ripristino di tutti i sistemi informatici oggetto dell’attacco hacker del 28 novembre scorso;
- le implicazioni cybercriminali dei dati illecitamente sottratti sono molteplici e vanno dalla vendita degli stessi, a soggetti di pochi scrupoli, fino alla possibilità di veri e propri furti di identità ai danni dei cittadini;
- come dimostrato ormai dai diversi *data breach*, che si sono susseguiti negli ultimi mesi, il settore sanitario è, inequivocabilmente, sempre più nell’interesse del cyber crimine, infatti, l’ultimo rapporto dell’Associazione italiana per la sicurezza informatica (Clusit), evidenzia come quello della sanità sia stato il secondo settore più colpito dagli attacchi informatici in Italia nel 2022, con una crescita del 16% rispetto al 2021;
- la Regione Emilia-Romagna definisce e approva, su proposta del Comitato ICT e in coerenza con il Piano Pluriennale per lo Sviluppo ICT del Servizio Sanitario Regionale, il “*Programma annuale delle attività da affidare a Lepida*” e tale Programma delinea gli ambiti progettuali e i servizi ICT di interesse del sistema sanitario e socio-sanitario regionale, gli obiettivi relativi e l’entità delle risorse finanziarie necessarie e disponibili, quindi, Lepida svolge un ruolo centrale in tale settore, tanto da autodefinirsi nel proprio Piano Industriale 2022 “*motore per l’attuazione ... del Piano ICT del Sistema Sanitario Regionale*” e la Regione Emilia-Romagna è socio di maggioranza di Lepida S.c.p.a. che controlla con il 95,64% del capitale sociale e che, per il restante 4,36%, è detenuto da altri 439 enti pubblici del territorio regionale.

Interroga la Giunta regionale per sapere:

1. quali le cause esatte di quanto accaduto e se siano state riscontrate mancanze o inefficienze, in particolare degli enti del SSR coinvolti, di Lepida e della Regione Emilia-Romagna;
2. se quanto successo il 28 novembre scorso, considerato che Lepida è coinvolta nella gestione delle piattaforme applicative: Accesso unitario Anagrafe Regionale Assistiti (ARA), Anagrafe Vaccinale Regionale (AVR), Cartella Clinica Assistenziale (CCA), Cartella SOLE, Centro Unico Prenotazione (CUP), Docer, Fascicolo Sanitario Elettronico (FSE), Federa, Icarer, Infrastruttura SOLE, LepidaID, Payer, Sistema Accoglienza Regionale (SAR), Sistema Informativo Sanità Penitenziaria (SISP), debba portare a prendere iniziative di ulteriori e urgenti azioni di salvaguardia dei dati personali dei cittadini;
3. se, considerato il ritardo nel ripristino dei servizi, ancora ad oggi non concluso, ciò non implichi che i Piani di Continuità Operativa, di Disaster Recovery aziendali di Lepida, nonché la stessa *Procedura per la gestione degli incidenti di sicurezza delle informazioni* di Lepida e delle aziende sanitarie coinvolte non si siano dimostrati inefficaci e, quindi, debbano essere radicalmente rivisti;
4. quali le conseguenze sulla salute dei cittadini causate dalla non erogazione o ritardata erogazione di prestazioni e servizi sanitari e quali le azioni per ridurre al minimo gli impatti;
5. se il *“Tavolo regionale per il coordinamento delle misure in materia di protezione dei dati personali delle Aziende sanitarie e degli Enti del SSR”*, costituito il 6 ottobre 2023, si sia riunito, in quali date e con quali risultati;
6. se sia stata fornita idonea comunicazione agli interessati rispetto alla pubblicazione dei loro dati e in quanti casi esattamente ciò sia avvenuto;
7. quali le risultanze delle analisi del contenuto dei file pubblicati, in termini numerici e in termini di natura esatta delle tipologie di dati pubblicati;
8. se la Regione intenda rivedere, razionalizzare ed eventualmente aumentare i propri investimenti in materia di protezione dei sistemi informatici, in particolare del settore sanitario e della conseguente formazione del personale;
9. se la gravità di quanto accaduto, che arriva a toccare i diritti e le libertà di tutti i cittadini coinvolti, porterà la Regione Emilia-Romagna a rivedere l'approccio verso questa tematica, in particolare, per il settore del Servizio Sanitario Regionale e relativamente al ruolo di Lepida S.c.p.a..