Provvedimento del 29 aprile 2025 [10134827]

[doc. web n. 10134827]

Provvedimento del 29 aprile 2025

Registro dei provvedimenti
n. 271 del 29 aprile 2025

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il dott. Claudio Filippi - il segretario generale reggente;

VISTO 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, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore l'avv. Guido Scorza;

PREMESSO

1. Introduzione.

In data 19 ottobre 2023, l'Ordine degli Psicologi della Regione Lombardia (di seguito, l'"Ordine") ha notificato all'Autorità, ai sensi dell'art. 33 del Regolamento, una violazione di dati personali, avvenuta il 3 ottobre 2023, riguardante un "accesso abusivo alla rete informatica, cifratura dati sui server e cancellazione dati da NAS di backup" (v. notifica del 19 ottobre, sez. F, punto 8).

Successivamente, in data 20 novembre 2023, l'Ordine ha integrato la predetta notifica, dichiarando di essere stato vittima di "un sofisticato attacco ransomware dall'associazione criminale NoEscape [che] ha comportato l'accesso abusivo alla rete informatica dell'Ordine, la cifratura dei dati e la successiva cancellazione dei backup che sono stati tuttavia recuperati successivamente […] in data 10.10.2023 quando il Titolare è venuto a conoscenza della fonte "malevola" delle anomalie riscontrate nei giorni precedenti, […] a seguito del ricevimento di una e-mail da parte di csirt@pec.acn.gov.it che indicava il riferimento a un link su Onion che rimandava a una pagina dove si minacciava la pubblicazione di 7GB di dati […]. Successivamente, a seguito del mancato pagamento del riscatto, i cyber criminali in data 18 ottobre e 31 ottobre 2023 hanno pubblicato sul dark web i dati esfiltrati".

L'Ordine ha a tal riguardo affermato di poter "escludere la perdita di integrità e disponibilità dei dati [in quanto] tutti gli archivi, sono stati completamente ripristinati grazie ai salvataggi eseguiti nel cloud di [un fornitore] e alla presenza di backup su dischi esterni USB conservati in cassaforte. Inoltre, […] l'agente malevolo è stato in grado di criptare ed esfiltrare solamente 6,9GB (compressi 4,5 GB): tale quantitativo è solamente di piccola entità rispetto alla dimensione e mole complessiva dei dati contenuti negli archivi dell'Ordine che corrisponde a centinaia di GB, i quali non sono stati impattati. Infatti, sono state impattate solo alcune cartelle contenenti file, non la totalità delle stesse. […] Il Titolare inoltre non ha evidenza che altri dati, diversi da quelli pubblicati sul dark web, siano stati oggetto di accesso da parte dei cyber criminali e questi nelle comunicazioni hanno sempre fatto riferimento unicamente ai dati poi pubblicati sul dark web" (v. notifica del 20 novembre, sezz. F, punto 7 e G, punto 1.4).

L'Ordine ha, altresì, rappresentato che gli interessati coinvolti nell'attacco informatico sono stati 3.000 e che l'"impatto della violazione [….] è alt[o] con esclusivo riferimento ai dati di [interessati coinvolti in] […] procedimenti disciplinari e alle persone citate negli stessi procedimenti, che rappresentano solo una parte molto limitata dei dati violati" - quantificando tali procedimenti in 159, "di cui la maggior parte riguardano gli ultimi due anni" -, mentre "per altri procedimenti più risalenti, la documentazione riguarda unicamente le parti coinvolte e il provvedimento adottato". L'Ordine ha, invece, ritenuto "in relazione ai dipendenti e i soli tre collaboratori del Titolare i cui documenti di identità sono stati esfiltrati, […] che la gravità [fosse] media" (v. notifica del 20 novembre 2023, sezz. F, punto 13, e G, punto 3).

Dalla documentazione in atti emerge che la violazione ha coinvolto circa 15.000 registrazioni di dati personali, fra cui dati anagrafici, di contatto, di pagamento, relativi a documenti d'identità/riconoscimento, coperti da segreto professionale, nonché dati appartenenti a categorie particolari (cfr. art. 9 del Regolamento e 2-sexies del Codice), quali dati che rivelano l'origine razziale o etnici, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la vita sessuale o l'orientamento sessuale, lo stato di salute, nonché dati relativi a condanne penali e reati (cfr. art. 10 del Regolamento e 2-octies del Codice). Ciò con la conseguenza che gli interessati sono stati esposti, secondo quanto valutato dall'Ordine e dichiarato nelle notifiche della violazione, a rischi di perdita di controllo dei dati, discriminazione, furto d'identità, frodi, pregiudizio alla reputazione, conoscenza da parte di terzi non autorizzati e danni economici e sociali significativi.

Con riferimento alle misure in essere al momento della violazione, l'Ordine ha dichiarato che esso effettuava "verifiche costanti sugli aggiornamenti dei sistemi operativi delle postazioni server e client, dei firmware degli apparati di rete [e che adottava un] sistema di autenticazione correttamente configurato e monitorato, antivirus […] su tutte le postazioni, salvataggi in locale su due NAS dislocati nelle due sedi, un backup in cloud […] nr. 5 HD USB in cassaforte presso la sede […] e due HD USB custoditi in cassetta di sicurezza presso la banca d'istituto" (v. notifica del 19 ottobre 2023, sez. F, punto 9). Inoltre, l'Ordine "aveva adottato le seguenti misure: (i) firmware degli apparati di rete, (ii) sistema di autenticazione correttamente configurato e monitorato, (iii) antivirus reset end point su tutte le postazioni, (iv) salvataggi in locale su due NAS dislocati nelle due sedi, (v) un backup in cloud con [un fornitore terzo], (vi) nr. 5 HD USB in cassaforte presso la

sede del Titolare e due HD USB custoditi in cassetta di sicurezza presso la banca d'istituto […;] una VPN (Virtual Private Network) per la connessione ai sistemi dell'Ordine. Tutte queste misure erano costantemente monitorate ed aggiornate". L'Ordine ha dettagliato tali misure con nota del 19 gennaio 2024 (pagg. 2 – 4).

Con riferimento alle misure adottate a seguito della violazione, l'Ordine ha rappresentato che "si è attivato per comprendere meglio l'accaduto e recuperare le copie di backup (fisiche e cloud) dei dati risiedenti sui propri server [, avendo] prontamente coinvolto nelle attività di ripristino [un fornitore terzo] […] e ha provveduto a (i) disabilitare sul firewall tutte le regole che permettevano di accedere dall'esterno in terminal server alla macchina XX che contiene il software dell'Albo degli psicologi, (ii) bloccare tutte le VPN attive e ad aggiungere delle regole che bloccassero ogni traffico da e verso la rete dalle 21.00 alle 7,00 di mattina, (iii) effettuare il cambio di password a partire dal server di dominio e poi ai server ESX che contengono le macchine virtuali. Nel frattempo, [si era] già provveduto a creare ex novo una macchina virtuale su cui è stato installato [un] software di backup […]. Una volta completata l'operazione è stato ripristinato il server virtuale che funge da Domain Controller, utilizzando una copia di backup presente su un disco fisico chiuso in cassaforte con data backup 31.07.2023. Grazie ad alcuni backup in cloud presso [un fornitore terzo] e alcuni dischi fisici di backup in cassaforte e nella cassetta di sicurezza presso la banca di riferimento dell'Ordine, il Titolare è riuscito a ripristinare i dati recuperando i dati cancellati grazie ai backup cloud e fisici, riportando la situazione al giorno prima dell'attacco. Pertanto, la perdita di disponibilità e integrità dei dati è stata solo temporanea grazie alle attività di ripristino completate. Inoltre, […] sono stati [poi] effettuati dei test al fine di comprendere le anomalie riscontrate e la natura dell'evento [, installando] un apposito software di monitoraggio in tutte le macchine, ivi inclusi i propri server. Successivamente, [si è] provveduto a 1. ripristinare con successo i dati, consentendo inoltre l'utilizzo delle applicazioni in cloud; 2. ripristinare il server XX ovvero il file server del Titolare; 3. riallineare i pc degli utenti non presenti nei giorni precedenti, recuperare i backup NAS presenti in sede, cambiare le password dei nuovi utenti; 4. dopo aver ottenuto una conferma [del fornitore terzo] circa il fatto che, una volta effettuata la copia di tutti i dati, il Titolare poteva provvedere all'eliminazione dei file criptati, (i) eliminare i file criptati del server presso la Casa della Psicologia dopo copia su NAS, e (ii) iniziare la creazione di una nuova macchine virtuale sul server ESX della Casa della Psicologia. Quando i dati sono stati pubblicati sul dark web, il Titolare ha effettuato delle attività di verifica on-line, anche nel dark web, cercando di identificare l'eventuale presenza di dati riconducibili agli archivi oggetto di cifratura e cancellazione e a ricostruire i dati personali impattati" (v. notifica del 20 novembre 2023, sez. H, punto 1).

In relazione alle misure tecniche e organizzative adottate per prevenire simili violazioni in futuro, l'Ordine ha dichiarato che "dopo aver ripristinato i dati e cancellato le copie criptate […] ha implementato misure quali: (i) la creazione degli accessi alla VPN con certificati al posto dei vecchi utenti locali, (ii) svolgimento di test di funzionamento, e (iii) modifica regole di collegamento degli utenti VPN sulla rete dell'Ordine, limitandone l'accesso ai soli server necessari. Inoltre, è stato installato il nuovo agent di backup [...] sul server XX ed è stata effettuata la riconfigurazione del backup sia sul cloud […] che sui 4 NAS […] [.L'Ordine] sta provvedendo alla adozione di un nuovo applicativo in cloud per la gestione dell'albo degli iscritti all'ordine ed è in corso di valutazione l'acquisto di un applicativo che oltre a raccogliere i file di log svolge anche funzione di analisi e prevede l'invio di alert all'ADS […] [.I] referenti IT del Titolare hanno ripristinato tutti gli archivi e stanno predisponendo un piano di ottimizzazione delle misure idonee che già erano in essere presso la struttura informatica dell'ordine adottando misure più stringenti in riferimento alle categorie di dati particolari quali l'adozione di un sistema di autenticazione a più fattori (MFA) e la cifratura degli archivi. Sono in corso di valutazione l'adozione di un software di monitoraggio […per] identificare situazioni di potenziale criticità e allertare gli ADS e una soluzione che consenta di garantire l'integrità dei salvataggi on site e un ripristino rapido dei dati, oltre alle misure già adottate […]" (v. notifica 20 novembre 2023, sez. H, punto 2).

Per quanto attiene alla comunicazione della violazione agli interessati, l'Ordine, in sede di notifica integrativa, ha rappresentato che avrebbe effettuato le comunicazioni agli interessati "entro il 24/11/2023 […] per i segnalanti/segnalati e individui citati nei procedimenti" e che avrebbe effettuato tali comunicazioni "anche a beneficio dei dipendenti e dei 3 collaboratori sopra citati a titolo precauzionale". In particolare, l'Ordine ha rappresentato la propria intenzione di inviare "una comunicazione via e-mail con riferimento ai segnalanti e segnalati relativi ai procedimenti dal 2018 ad oggi che possano essere ragionevolmente tracciabili" e ha dichiarato che "la violazione verrà comunicata direttamente a 334 interessati (numero che include i soggetti rintracciabili coinvolti nei procedimenti disciplinari, 13 dipendenti e 3 fornitori)", mentre "in relazione agli altri interessati, il Titolare pubblicherà una comunicazione pubblica sul proprio sito Internet in quanto in conformità con l'articolo 34, comma 3, del Regolamento […] l'invio di una comunicazione all'interessato richiederebbe sforzi sproporzionati". A tal riguardo, sono state prodotte le tre tipologie di comunicazioni: "1. Comunicazione individuale per i segnalanti e segnalati dei procedimenti disciplinari che sono identificabili; 2. Comunicazione pubblicata sul sito in relazione agli individui a cui non è possibile inviare una comunicazione; 3. Comunicazione individuale per i dipendenti e ai 3 collaboratori i cui documenti di identità sono stati esfiltrati" (v. notifica del 20 novembre 2023, sez. L, punti 3 e 4).

L'Ordine ha, infine, dichiarato di aver provveduto a comunicare agli interessati l'occorsa violazione di dati personali, ai sensi dell'art. 34 del Regolamento, "in data 23.11.2023 – agli interessati che presentavano un alto livello di rischio con riferimento all'Incidente, i.e. i segnalati e i segnalanti nell'ambito dei procedimenti disciplinari nonché i dipendenti dell'Ordine" (v. nota del 19 gennaio 2024, pag. 11), mediante una comunicazione su base individuale, e "in relazione agli altri interessati [mediante] una comunicazione pubblica sul proprio sito Internet in quanto in conformità con l'articolo 34, comma 3, del Regolamento […] l'invio di una comunicazione all'interessato richiederebbe sforzi sproporzionati" (v. notifica del 20 novembre 2023, sez. L, punto 3).

In relazione alla violazione di dati personali in questione sono stati presentati al Garante due reclami ai sensi dell'art. 77 del Regolamento e una segnalazione ai sensi dell'art. 144 del Codice.

2. L'attività istruttoria.

In riscontro a una richiesta d'informazioni dell'Autorità (nota prot. n. 0168453/23 del 21 dicembre 2023), l'Ordine, con nota del 19 gennaio 2024 (prot. 0001441), ha integrato le informazioni circa le misure tecniche e organizzative poste in essere per prevenire simili violazioni in futuro, rappresentando di aver "adottato un piano", che prevede l'installazione di un "software tool per la rilevazione di minacce alla sicurezza dei dati […; una] nuova segmentazione della rete [per] rafforzare la propria protezione contro cyber attacchi [,] isolare eventuali attacchi ed evitare che si diffondano sulla rete e contagino altri server e dispositivi […]; nuove procedure di backup e air-gap tra produzione e backup", evidenziando "l'affidabilità del sistema "multi-livello" di backup dei dati" in essere al momento della violazione (v. nota del 19 gennaio 2024, pagg. 4 - 5).

A seguito di un'ulteriore richiesta d'informazioni dell'Autorità (nota prot. n. 0067836/24 del 4 giugno 2024), l'Ordine, con nota del 19 giugno 2024 (prot. n. 0009014), ha fornito copia di un'analisi svolta da un consulente esterno, da cui è emerso che "il gruppo NoEscape ha pubblicato sul loro leak site un archivio 7zip diviso in tre parti […] [e che] la dimensione dei 5 dati pubblicati ammonta a 4.16GB e contiene: Carte d'identità e passaporti; Accordi riservati; Contratti; Documenti bancari; Dati correlati ai propri clienti; Report interni" (v. Incident Response Report (IR) - v.1.1, allegato alla nota del 19 giugno 2024, pag. 20 – di seguito "report incidente").

Con nota del 16 ottobre 2024 (prot. n. 0120794), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato all'Ordine, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, per aver omesso di adottare misure

adeguate a rilevare tempestivamente le violazioni di dati personali e garantire la sicurezza degli stessi, in violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento. Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del 15 novembre 2024, l'Ordine, per il tramite dei propri avvocati, ha presentato una memoria difensiva, dichiarando, in particolare, che:

- "l'Ordine - nonostante le significative restrizioni di carattere economico [...-] ha implementato le proprie misure di sicurezza in conformità alle linee guida dell'Agenzia per l'Italia Digitale ("AgID") di cui alla Circolare n. 2/2017 del 18 aprile 2017 [...] relative alle "misure minime di sicurezza ICT per le pubbliche amministrazioni" [...] [, fermo restando che] l'Ordine aggiorna periodicamente queste misure, al fine di garantire un livello di sicurezza informatica adeguato e in linea al progressivo sviluppo tecnologico";

- "il combinato disposto degli artt. 5, par. 1, lett. f) e 32, par. 1, del Regolamento prevede [...] non [prevede] un numerus clausus di misure che debbano essere adottate perentoriamente [...]. Al contrario, l'implementazione di specifiche misure di sicurezza dipende dal livello di rischio posto dal trattamento in concreto, nonché dall'evoluzione tecnologica del settore e dai costi di attuazione e dalle risorse effettivamente disponibili per la loro attuazione";

- "nel caso delle pubbliche amministrazioni, però, un'indicazione sulle misure di sicurezza attese è fornita dalla Circolare AgID che prevede i seguenti tre livelli di sicurezza: "minimo" [...]; "standard", che può essere assunto come base di riferimento per la maggior parte delle pubbliche amministrazioni; "alto" [...]";

- "l'Ordine, in qualità di ente pubblico non economico – e dunque di pubblica amministrazione ai sensi del D. Lgs. 165/2001 soggetta alla competenza di AgID – ha adottato le proprie misure di sicurezza in linea con le disposizioni della Circolare AgID, conformandosi al livello standard di cui alla lettera b) [...]";

- "tale livello di sicurezza è da ritenersi adeguato considerato il livello di rischio effettivo per i sistemi dell'Ordine alla luce delle seguenti circostanze: a) le attività svolte dall'Ordine non rientrano nella definizione di servizi essenziali per i cittadini di cui alla Circolare AgID; b) sotto il profilo organizzativo, l'Ordine non rientra tra le pubbliche amministrazioni che, per dimensioni e capacità economica, presenta[no] un elevato livello di rischio";

- "[...] l'Ordine è un ente pubblico non economico dalla limitata capacità di sostentamento con soli 13 dipendenti. L'Ordine non riceve sussidi statali e le sue risorse economiche derivano dai soli pagamenti effettuati dagli iscritti. Ciononostante, [...] l'Ordine ha sempre posto particolare attenzione al tema della sicurezza informatica, destinando in media il 5-7% del proprio fatturato annuale alla gestione delle sue risorse ed infrastrutture tecnologiche [...] in linea con lo standard di mercato [...]";

- "pertanto, l'adozione di misure di livello superiore avrebbe comportato un onere sproporzionato a carico dell'Ordine [...]";

- "rispetto alla mancata adozione di un idoneo meccanismo c.d. di alert per l'identificazione tempestiva di eventuali anomalie sui sistemi dell'Ordine, si precisa [...] [che...] l'Ordine aveva già implementato [un] firewall [...] a protezione del proprio perimetro aziendale, il quale è in grado di rilevare i logs e i tentativi di connessione RDP (Remote Desktop Protocol) dall'esterno, inclusi eventuali tentativi di accesso indebito alla rete aziendale. In particolare, i log raccolti dal firewall venivano archiviati sui server dell'infrastruttura

dell'Ordine e inviati a un meccanismo di archiviazione […] al fine di avere una doppia copia dei log. Il controllo di tali log, inoltre, era affidato ai dipendenti dell'Ordine, che monitoravano periodicamente i log del firewall al fine di individuare eventuali accessi sospetti";

- "tali presidi risultavano, dunque, nel loro complesso idonei ad individuare tempestivamente una violazione di dati per due ragioni principali […, essendo] in linea con la Circolare AgID che, per la tempestiva identificazione delle violazioni, ritiene sufficiente l'adozione di – inter alia – misure che prevedono la registrazione di qualsiasi anomalia rispetto al normale traffico di rete per consentirne l'analisi off line. Infatti, secondo l'AgID, l'adozione di meccanismi di DLP (Data Loss Prevention) in grado di individuare autonomamente situazioni sospette e di inviare un alert è da ritenersi una misura di livello alto a cui l'Ordine non è chiamato a conformarsi. Inoltre, l'adozione di un meccanismo c.d. di alert e di monitoraggio dei log più avanzato avrebbe richiesto un investimento, in termini di risorse economiche e lavorative, sproporzionato per l'Ordine";

- "[…] per garantire un monitoraggio costante degli alert rilevati, l'Ordine dovrebbe altresì disporre di personale qualificato in numero sufficiente a svolgere tale attività, anche nei fine settimana e in orario notturno";

- "in ogni caso, […] non appena verificatosi il Data Breach, l'Ordine ha avviato un processo volto ad incrementare il livello di sicurezza dei propri sistemi nei limiti in ogni caso delle risorse economiche a propria disposizione. In particolare: […] è stato installato [un] software [...] che consente di ricevere degli alert al variare di configurazioni di Active Directory o in caso di accessi a sistemi con utenze particolari";

- "[…] in virtù delle caratteristiche e delle modalità di svolgimento dell'attacco […], il meccanismo stesso non sarebbe risultato efficace ad impedire il verificarsi della violazione […] e/o a garantirne una più tempestiva individuazione. Il presupposto perché infatti possa funzionare il meccanismo di alert in esame è che gli attaccanti generino un traffico anomalo a causa del volume, della provenienza geografica o del periodo temporale degli accessi. Laddove tale traffico anomalo manchi, il meccanismo di alert non potrebbe dunque individuare situazioni sospette";

- "[…] l'attacco subito dall'Ordine [è] di tipo brute force (ovvero gli attaccanti hanno ripetutamente tentato l'accesso alle risorse informatiche dell'Ordine utilizzando le credenziali di accesso di alcuni utenti) […]";

- "[…] non sono stati registrati "picchi di traffico in uscita" tali da generare eventuali alert alla luce delle seguenti circostanze: a) i tentativi di connessione RDP (Remote Desktop Protocol) dall'esterno sono avvenuti nel fine settimana o durante orari serali; b) i tentativi di accesso non sono avvenuti in modo massivo, bensì distanziati tra loro nel tempo ed evitando l'accesso da paesi bloccati; c) gli attaccanti avevano a disposizione dei "sample" di file dell'organizzazione che hanno consentito loro di accedere ai sistemi con le credenziali dell'Ordine; e d) il traffico generato dagli attaccanti era sottosoglia, in quanto è stato quantificato in massimo 5GB, diviso in più giorni, mentre il traffico medio sui sistemi dell'Ordine è tra i 10 e i 20 GB, a seconda delle attività (anche di manutenzione e aggiornamento) effettuate giornalmente";

- "infatti, non è infrequente che, anche durante il fine settimana e in orari serali, l'Ordine svolga attività ed eventi che prevedono l'accesso ai sistemi. Di conseguenza, la mera presenza di traffico notturno o durante il fine settimana, tra l'altro sottosoglia, non poteva costituire indizio circa la presenza di accessi illegittimi, essendo plausibile che utenti legittimi fossero connessi alla rete dell'Ordine. Ciò senza considerare che una rilevazione di traffico anomalo non coincide necessariamente con una violazione dei dati personali in corso, che

potrebbe invece richiedere – come nel caso di specie – diverso tempo per essere confermata";

- "[…] grazie alle particolari tecniche elusive con cui l'attacco è stato perpetrato, gli attaccanti sarebbero comunque riusciti ad evitare [eventuali] meccanismi di alert […]";

- quanto alla "mancata adozione di un sistema di autenticazione a più fattori, si precisa che l'Ordine, al momento in cui si è verificato il data breach, aveva implementato un sistema di autenticazione correttamente configurato e monitorato, in linea con le disposizioni della Circolare AgID. A tal proposito, infatti, la Circolare AgID richiede l'implementazione di un doppio fattore di autenticazione come misura di livello c.d. "alto" (non "standard") solamente per le utenze privilegiate e l'attribuzione di diritti amministrativi, considerando equipollente l'alternativa misura di elevatezza delle password che […] è stata correttamente adottata dall'Ordine. In particolare, al tempo degli eventi, il sistema utilizzato per l'autenticazione degli utenti dell'Ordine e per l'accesso ai sistemi attestati al dominio (i.e. postazioni di lavoro e server) era basato su Active Directory di [denominazione azienda], mediante l'utilizzo della VPN (Virtual Private Network) […] di [denominazione azienda] per assicurare la sicurezza della connessione ai sistemi dell'Ordine. Inoltre, l'accesso al pc dell'utente avveniva tramite due passaggi, ossia l'inserimento della password di criptazione del disco, nonché delle diverse credenziali di dominio. Infine, apposite credenziali da utilizzare nei processi di autenticazione e autorizzazione informatica con riferimento ai server dati e di posta elettronica venivano assegnate ai dipendenti dell'Ordine. Non solo; le credenziali attribuite dovevano in ogni caso rispettare i requisiti di robustezza previsti dalla Circolare AgID. In particolare, le password dovevano essere di 14 caratteri e non potevano essere riutilizzate più volte. Infatti il sistema impedisce agli utenti di riutilizzare una password già utilizzata in passato per accedere allo stesso sistema informatico";

- "l'Ordine ha [ora] provveduto ad aggiungere una procedura di autenticazione informatica doppia basata su: (i) utilizzo di username e password (già presente); (ii) certificato con doppia autenticazione; e (iii) applicazione dell'attendibilità del dispositivo";

- "comunque, l'accesso da parte dei cybercriminali ai sistemi informatici non risulta avvenuto tramite la sottrazione di credenziali di accesso, ma piuttosto per un bug del sistema che è stato prontamente risolto dall'Ordine";

- quanto alla "inadeguata segmentazione e conservazione delle credenziali di autenticazione, non si rilevano ragioni per cui il meccanismo di segregazione implementato dall'Ordine sia da considerarsi non adeguato, né sul concreto ruolo che tale sistema avrebbe avuto nel contesto della Violazione di dati personali. Difatti, la Circolare AgID si limita a prevedere la conservazione delle credenziali in modo da "garantirne disponibilità e riservatezza" e, nel caso in cui per l'autenticazione si utilizzino certificati digitali, garantire una adeguata protezione alle chiavi private. Tali requisiti risultano, dunque, rispettati dall'Ordine";

- "di regola, la mancata segmentazione delle password o l'inadeguata conservazione delle stesse rilevano principalmente nel caso in cui l'attacco si verifichi attraverso l'introduzione nel sistema di un malware. In tal caso, la mancata segmentazione impedisce l'isolamento della minaccia comportando così potenzialmente la propagazione del malware su tutta l'infrastruttura informatica. Nel caso di specie, invece, il ransomware non si è propagato verso sistemi ulteriori, avendo l'Ordine bloccato l'attacco e la cifratura prima che questa potesse estendersi a server differenti da quelli verso cui era indirizzato l'attacco. Di conseguenza, la mancata segmentazione non ha avuto alcun impatto sull'attacco, non potendo dunque essere considerata contestabile la sua mancata adozione";

- “[…] in seguito al verificarsi del Data Breach, l'Ordine [ha] comunque provveduto ad introdurre una nuova ulteriore segmentazione di rete […che] consentirà di isolare eventuali attacchi [, di] evitare che si diffondano sulla rete e contagino altri server e dispositivi […e] di fare in modo che i dispositivi sulla rete di management non siano raggiungibili dalla rete LAN se non attivando delle regole sul firewall (solo in caso di necessità)”;

- quanto alla contestata “mancata protezione delle credenziali con algoritmi crittografici allo stato dell'arte […] è […] fondamentale chiarire che: (i) il dominio di posta elettronica “opl.it” e il dominio di Active Directory utilizzato per l’accesso ai server interni dell’Ordine risiedono su server diversi: il primo su server esterni all’Ordine (opl.it), mentre il secondo sui server interni dell’Ordine (opl.lan); (ii) l’analisi condotta ha riguardato solo quanto presente nel dark web e ha rilevato vulnerabilità nel solo dominio esterno dell'Ordine (opl.it); e (iii) le credenziali analizzate si riferiscono esclusivamente al dominio di posta elettronica e non consentono in alcun modo l’accesso ai sistemi interni dell’Ordine”;

- pertanto, “è del tutto irrilevante che alcune delle suddette credenziali fossero classificate con severità “critical” e “high”, dal momento che appartenevano a indirizzi di posta elettronica che non potevano comunque essere utilizzati per l’accesso ai sistemi interni dell'Ordine. Peraltro, solo 3 su 12 utenti risultavano essere dipendenti dell’Ordine, e nessuno di questi aveva una password classificata come “critical” o “high”. Molte delle credenziali esposte risultavano, infatti, obsolete o inventate […]. Di conseguenza, l’asserita mancata crittografia di tali credenziali risulta del tutto svincolata dalle dinamiche dell’attacco”;

- “[…] le credenziali utilizzate per l’accesso ai sistemi interni dell’Ordine erano protette da algoritmi crittografici allo stato dell’arte. Infatti, l’accesso ai server avveniva tramite Active Directory, il quale utilizza di default la crittografia. Infine, al fine di introdurre un elemento ulteriore di protezione, i dischi dei computer degli utenti erano criptati, richiedendo una ulteriore password iniziale per l’accesso. Tali misure di crittografia risultano in linea con la Circolare AgID, la quale prevede l’obbligo “di effettuare un’analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica””;

- “è opportuno osservare la non pertinenza del richiamo effettuato da codesta Autorità alle Linee Guida Funzioni Crittografiche – Conservazione delle Password adottate con provvedimento n. 594 del 7 dicembre 2023 [doc. web n. 9962283], in quanto ancora non adottate al momento in cui si sono verificati i fatti contestati”;

- “l'Ordine sta valutando l'adozione di un sistema di crittografia in linea con i requisiti previsti dal Garante, nonché dalla Direttiva UE 2022/2555”;

- “la condotta contestata […] (i) ha riguardato un numero esiguo di interessati e dati personali rispetto a quelli presenti nel sistema dell'Ordine (6,9 GB su un totale di 350 GB); (ii) ha generato un rischio elevato ad un numero limitato di interessati […] [e] l'Ordine ha notificato gli interessanti impattati da un rischio più elevato su base individuale, mentre per gli altri ha provveduto a pubblicare un annuncio liberamente consultabile sul proprio sito internet; (iii) ha comportato la sola perdita di confidenzialità, senza intaccare l'integrità e la disponibilità dei dati, la cui compromissione è stata solo temporanea grazie alle azioni intraprese dall'Ordine per limitare gli effetti negativi e alla presenza di backup delle informazioni; (iv) non ha significativamente impattato i sistemi dell'Ordine […]”;

- “al fine di migliorare la individuazione delle violazioni e la sicurezza dei sistemi, nonché per prevenire simili attacchi in futuro, l'Ordine ha provveduto a: (i) creare accessi VPN certificati; (ii) adottare un sistema di autenticazione a più fattori (MFA); (iii) definire password policy più stringenti; (iv) bloccare gli accessi notturni alla rete; (v) disattivare tutti gli ingressi ai server

ed inserire delle regole più rigide per l'accesso; (vi) controllare la geolocalizzazione degli accessi esterni; (vii) introdurre una ulteriore segmentazione della rete [… per] isolare nuovi eventuali attacchi ed evitare che si diffondano sulla rete e contagino altri server e dispositivi; (viii) riconfigurare gli switch di rete esistenti […]; (ix) limitare l'accesso in remoto tramite VPN […]; (x) implementare nuovi sistemi di backup immutabili […]; (xi) implementare un air-gap tra ambiente di produzione e backup […] (xiii) modificare le regole di collegamento degli utenti VPN, cifrare gli archivi e adottare un nuovo applicativo in cloud per la gestione dell'Albo";

- "[…] la gravità dell'impatto della violazione […] è alta con esclusivo riferimento ai soggetti cui riferiscono i procedimenti disciplinari esfiltrati e alle persone citate negli stessi procedimenti, che rappresentano solo una parte molto limitata dei dati ottenuti illecitamente (i.e. 159 procedimenti). In relazione ai dati personali dei dipendenti coinvolti nel Data Breach, invece, le uniche categorie particolari di dati personali impattate riguardano l'appartenenza sindacale di tali dipendenti per la presenza unicamente di ricevute di pagamento delle quote di adesione. Infine, per quanto riguarda le altre categorie di interessati coinvolte, in particolare i fornitori e gli altri iscritti all'Ordine non coinvolti in procedimenti disciplinari, le informazioni oggetto della violazione dei dati personali sono prevalentemente di pubblico dominio. In generale, quindi, il Data Breach non ha coinvolto i dati maggiormente sensibili trattati dall'Ordine".

In occasione dell'audizione, richiesta ai sensi dell'art. 166, comma 6, del Codice e tenutasi in data 2 dicembre 2024 (v. verbale prot. n. 0141629 della medesima data), l'Ordine, rappresentato dai propri avvocati, ha dichiarato, in particolare, che:

- "l'attacco […] era particolarmente sofisticato ed elusivo e, pertanto, nemmeno adottando sistemi di allerta più avanzati sarebbe stato possibile rilevarlo; in particolare, l'esfiltrazione dei dati (circa 5 GB) è avvenuta in maniera progressiva, in orario notturno e in giorni festivi, senza mai superare la soglia di traffico giornaliero media (circa tra 10 e 20 GB)";

- "sebbene non ci siano specifiche evidenze, le circostanze dell'attacco sembrano suggerire che lo stesso fosse mirato a ottenere specifici dati e documenti e commissionato da soggetti non identificati che avevano interesse a entrare in possesso di tali dati e documenti o comunque a causare un danno all'Ordine che impattasse gli stessi, avendo, peraltro, i soggetti in questione verosimilmente conoscenza dei sistemi informatici dell'Ordine (es. soglia di traffico medio)";

- "quanto alle misure adottate per assicurare la sicurezza delle password, che l'Ordine ritiene fossero comunque adeguate, deve evidenziarsi che, per quanto sopra detto in merito alle ridotte dimensioni dell'Ordine e alle scarse risorse economiche e organizzative, l'Ordine non poteva permettersi di effettuare attività come ad esempio, vulnerability assessment e penetration test, oppure verifiche nel dark web volte a controllare in via preventiva l'eventuale perdita di confidenzialità di credenziali";

A scioglimento di una specifica riserva formulata nel corso dell'audizione, l'Ordine, sempre per il tramite dei propri avvocati, con nota dell'11 dicembre 2024, ha dichiarato, in particolare, che:

- sebbene in sede di memoria difensiva l'Ordine abbia dichiarato che "l'accesso da parte dei cybercriminali ai sistemi informatici non risulta avvenuto tramite la sottrazione di credenziali di accesso, ma piuttosto per un bug del sistema che è stato prontamente risolto dall'Ordine […,] è opportuno chiarire che, da un punto di vista meramente tecnico-informatico, il termine "bug" è stato utilizzato nella memoria per una "vulnerabilità" dei sistemi che i cybercriminali hanno sfruttato per potervi accedere illegittimamente e agevolmente";

- “nello specifico, il vettore compromesso e utilizzato dagli attaccanti risulta essere "il server XX" – che esponeva il servizio di Remote Desktop Protocol ("RDP") – dal quale risultano connessioni dall'esterno durante tutto l'attacco (i.e., dal 30 settembre 2023 al 3 ottobre 2023), con scansioni per rilevare la presenza di eventuali vulnerabilità. Tuttavia, le prime richieste di connessione sono risultate come dei tentativi falliti di accesso all'RDP. Gli accessi sono, invece, effettivamente avvenuti nella fase finale dell’attacco (i.e., dalle 23.12 del 2 ottobre 2023 alle 04.01 del 3 ottobre 2023)”;

- “il sistema RDP è un sistema che consente l'accesso da remoto a un computer o a un server in esecuzione sulla stessa rete locale LAN, permettendo agli utenti autorizzati di visualizzare lo schermo e interagire con il sistema come fossero fisicamente presenti. Tuttavia, per abilitare tali connessioni da remoto, la RDP richiede l'apertura di porte aperte e pubblicamente visibili. Tale caratteristica espone ad accessi RDP dall'esterno da parte di soggetti non autorizzati”;

- “nel caso di specie, da quanto emerge dall'Incident Response Report […], deve ritenersi che gli attaccanti abbiano: (i) individuato la vulnerabilità del server che esponeva il servizio di RDP tramite scansioni attive da parte di agenti automatizzati o bot; e (ii) tentato di accedere al sistema sfruttando credenziali ottenute presumibilmente dal dark web o attraverso altri strumenti automatizzati utilizzati al fine di effettuare tentativi ripetuti di accesso che generano combinazioni casuali di nomi utente e password fino ad individuarne una valida (c.d. brute force attack)”;

- “in ogni caso, è da escludere che l'origine della Violazione di dati personali sia da rinvenirsi esclusivamente nelle credenziali esposte relative al dominio "opl.it" […] in quanto le credenziali sottratte si riferiscono unicamente al dominio di posta elettronica e non permettevano in alcun modo l'accesso al sistema RDP dell'Ordine (che, invece, è il sistema a cui hanno avuto effettivamente accesso i cybercriminali)”;

- “il dominio di posta elettronica “opl.it” e il dominio di Active Directory utilizzato per l’accesso ai server interni dell’Ordine risied[o]no su server diversi […]; (ii) l’analisi condotta ha rilevato vulnerabilità nel solo dominio esterno dell'Ordine (opl.it); e (iii) le credenziali utilizzate sono indirizzi e-mail che, in alcuni casi, non sono neppure associati ad un valido account. Infatti, solo 3 su 12 indirizzi risultano riferibili a dipendenti dell’Ordine, mentre molte delle credenziali esposte risultavano obsolete o inventate […], e comunque non utilizzabili per l’accesso all'RDP che risulta essere il sistema a cui gli attaccanti hanno effettivamente avuto accesso”;

- “le analisi effettuate sugli elementi e i logs resi disponibili dal referente tecnico dell’organizzazione hanno permesso di identificare il probabile vettore di ingresso, nello specifico un server che esponeva il servizio di Remote Desktop";

- “alla luce di quanto sopra, l'accesso ai sistemi informatici dell'Ordine è avvenuto a causa di una vulnerabilità di un punto di accesso RDP dell'infrastruttura dell'Ordine, sebbene gli attaccanti abbiano tentato di utilizzare credenziali che, con ogni probabilità, erano già in loro possesso (verosimilmente tramite il dark web) o generate attraverso un attacco di tipo brute force”;

- “tuttavia, le credenziali sottratte non consentivano di accedere alla rete dell'Ordine (ovvero al sistema RDP esposto). Quindi, anche qualora l'Ordine avesse adottato soluzioni di autenticazione a più fattori, questo non avrebbe evitato il verificarsi della Violazione di dati personali”;

- “in ogni caso, le condizioni economiche dell'Ordine non consentivano di poter sostenere il

costo di un servizio di scansione del dark web per l'identificazione di credenziali sottratte e l'esecuzione di periodici vulnerability assessment e penetration test".

3. Esito dell'attività istruttoria.

3.1 La normativa in materia di protezione dei dati personali.

Ai sensi dell'art. 5, par. 1, lett. f), del Regolamento, il trattamento di dati personali deve essere effettuato in conformità al principio di "integrità e riservatezza", in base al quale i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Sulla base di tale principio, l'art. 32 del Regolamento prevede che il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio. Il titolare è il soggetto responsabile dell'attuazione di tale misure e deve essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (v. artt. 5, par. 2, e 24 del Regolamento; cfr. le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. punto 41).

3.2 La mancata adozione di misure adeguate a rilevare le violazioni dei dati personali.

Come risulta dalla documentazione in atti, dalle "analisi preliminari sui logs del FireWall […] installato a protezione del perimetro aziendale, [è stato rilevato] quanto segue: durante il periodo compreso tra il 30 settembre e il 1° ottobre 2023, sono stati rilevati numerosi tentativi di connessione RDP (Remote Desktop Protocol) dall'esterno, indirizzati alla macchina "XX" e "XX" […] [e che] dal 2 ottobre, vengono registrate sessioni RDP negli orari serali perdurate fino al 3 ottobre, suggerendo, quindi, una minaccia persistente […] risulta[ndo] quindi probabile che le attività non legittime [fossero] iniziate in data 30 settembre 2023 e terminate la mattina del 03 ottobre 2023 con l'esecuzione del Ransomware (cfr. Incident Response Report (IR) - v.1.1 allegato alla nota del 19 giugno 2024, pagg. 8 - 9).

Soltanto "il giorno 3.10.2023, a seguito della ricezione di alcune segnalazioni provenienti da utenti dell'Ordine che riferivano l'impossibilità di accedere alla rete", l'Ordine si è accorto della criptazione di alcuni server e della cancellazione dei dati di backup, ritenendo "inizialmente che la stessa fosse conseguente ad un problema tecnico". Successivamente, solo "a seguito di una approfondita analisi condotta da parte dell'amministratore di Sistema (ADS) conclusasi il 10.10.2023, è stato possibile per il Titolare comprendere che l'Incidente rappresentava una violazione dei dati personali ai sensi del Regolamento (pur non avendo ancora effettiva cognizione del livello di serietà della stessa)" (Incident Response Report (IR) - v.1.1 allegato alla nota del 19 giugno 2024, pagg. 8).

L'Ordine non aveva, pertanto, adottato alcuna misura adeguata a rilevare tempestivamente le violazioni dei dati personali sulla base di comportamenti anomali risultanti dagli accessi alla rete aziendale (quali, a esempio, l'orario e la frequenza degli accessi, tendenzialmente notturni, la loro provenienza da indirizzi IP di paesi stranieri) e dalle operazioni effettuate con gli account di dominio con o senza privilegi amministrativi (quali, a esempio, la disattivazione di misure di sicurezza o la terminazione di processi e servizi), anche in ragione del fatto che "per garantire un monitoraggio costante degli alert rilevati, l'Ordine dovrebbe altresì disporre di personale qualificato in numero sufficiente a svolgere tale attività, anche nei fine settimana e in orario notturno" (nota del 15 novembre 2024, cit.).

Quanto alle difese prospettate dall'Ordine successivamente alla contestazione di violazione amministrativa, deve osservarsi che, come anche di recente ribadito dal Garante (v. provv.ti 17 luglio 2024, n. 444, doc. web n. 10057610), la circostanza che l'Ordine avesse "adottato le proprie misure di sicurezza in linea con le disposizioni della Circolare AgID, conformandosi al livello standard", non esonera, in generale, il titolare del trattamento dall'obbligo di effettuare una valutazione, in concreto, sull'appropriatezza delle misure adottate per garantire la sicurezza del trattamento, tenendo conto del contesto in cui si opera. In particolare, l'adozione delle misure indicate nelle predette linee guida – che costituiscono, peraltro, le "misure minime di sicurezza per la pubblica amministrazione italiana, avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche" - non garantisce, di per sé, il rispetto degli obblighi in materia di sicurezza. Le predette linee guida hanno, infatti, lo scopo di "indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i loro sistemi informativi", prendendo le mosse "dall'insieme di controlli noto come SANS 20 […] nella versione 6.0 di ottobre 2015", e "assicurare il minimo livello di protezione nella maggior parte delle situazioni […] avendo ben presente le enormi differenze di dimensioni, mandato, tipologie di informazioni gestite, esposizione al rischio, e quant'altro caratterizza le oltre ventimila amministrazioni pubbliche", raccomandando a "ogni amministrazione […] di individuare [al proprio] interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali […] applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi". Nello specifico, le Linee guida, essendo state emanate sulla base dello stato dell'arte, delle conoscenze tecniche e delle minacce cibernetiche presenti nel 2015, non potevano tener conto dell'aggravarsi del rischio cibernetico negli ultimi anni, anche a causa della diffusione e adozione, durante la pandemia COVID-19, di modalità e strumenti tecnologici per consentire lo svolgimento delle attività (lavorative e non) a distanza. Tale cambio di scenario, visto anche l'aumento significativo degli attacchi da parte dei cybercriminali, avrebbe richiesto una rinnovata valutazione che ponderasse i nuovi e ben più gravi rischi connessi al trattamento per i diritti e le libertà degli interessati in relazione all'adeguatezza delle misure adottate. La predetta valutazione, non potendo essere cristallizzata e, quindi, conclusa al momento in cui i trattamenti sono stati progettati, avrebbe dovuto essere periodicamente effettuata nel corso del tempo, anche alla luce dello sviluppo tecnologico; ciò anche al fine di maturare una consapevolezza in ordine alla necessità di attenuare i rischi derivanti da violazioni di dati personali. Pertanto, l'asserita conformità alle misure indicate nelle predette Linee guida di Agid non esaurisce l'obbligo del titolare del trattamento di adottare misure adeguate sulla base di una propria valutazione del rischio. Infatti, il Regolamento, in ossequio al principio di responsabilizzazione, demanda al titolare il compito di individuare e adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dai trattamenti, che, nel caso di specie, risultavano particolarmente elevati in ragione della natura dei dati trattati, del numero elevato di interessati, tra cui soggetti vulnerabili, nonché, in caso di violazione, delle possibili conseguenze negative per gli interessati in caso di compromissione della riservatezza dei dati.

Non può essere, inoltre, accolto l'argomento difensivo prospettato dall'Ordine, in base al quale, tenuto conto del fatto che l'attacco informatico in questione era particolarmente sofisticato (esfiltrazione dei dati in maniera progressiva in orario notturno e in giorni festivi, senza mai superare la soglia di traffico media), eventuali meccanismi di alert in tempo reale per l'identificazione tempestiva di eventuali anomalie sarebbero stati, in ogni caso, inefficaci. Tali meccanismi automatici, ove opportunamente configurati e presidiati, consentono, infatti, di rilevare eventi che, proprio per le particolari accortezze impiegate dagli attaccanti, possono sfuggire al controllo umano, mettendo in rilevo determinati eventi (es. traffico in orario notturno o in giorni festivi, in giorni in cui non sono previsti interventi di manutenzione programmati) ancorché non significativi sul piano statistico (es. traffico in linea con la soglia di traffico medio giornaliero).

Né può assumere rilevanza la circostanza che, come sostenuto dall'Ordine, l'adozione dei predetti sistemi automatizzati di alert avrebbe comportato un costo economico elevato e sproporzionato in capo all'Ordine, essendo lo stesso un Ente pubblico dotato di limitate risorse organizzative e finanziarie.

Al riguardo, deve considerarsi che l'art. 32 del Regolamento menziona i "costi di attuazione" soltanto tra i fattori che il titolare del trattamento deve tenere in considerazione ai fini dell'individuazione delle misure tecniche e organizzative adeguate a fronteggiare i rischi che insistono sui dati oggetto di trattamento (cfr. art. 24 del Regolamento). Tale fattore "implica che il titolare non impieghi una quantità sproporzionata di risorse nel caso in cui esistano misure alternative, meno dispendiose, ma efficaci", fermo restando che "il costo di attuazione rappresenta un fattore di cui tenere conto nel realizzare la protezione dei dati fin dalla progettazione, e non già un motivo per astenersi dal realizzarla"; pertanto, "le misure individuate devono […] garantire che l'attività di trattamento prevista dal titolare non comporti trattamenti di dati personali in violazione dei principi, indipendentemente dal costo di tali misure. I titolari devono essere in grado di gestire i costi complessivi per poter attuare efficacemente tutti i principi e, di conseguenza, tutelare i diritti" (Comitato europeo per la protezione dei dati, "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate il 20 ottobre 2020, parr. 24 e 25; cfr. anche ENISA, "Guidelines for SMEs on the security of personal data processing", del dicembre 2016, pag. 12, ove si evidenzia che "il riferimento […] ai costi di implementazione non deve essere interpretato come una scusa per non agire, ma piuttosto come un invito a tutte le parti interessate a semplificare e ridurre i costi. In questo senso, l'approccio alla semplificazione della nozione di rischio e l'adozione di misure adeguate sono fondamentali per la corretta attuazione di questo articolo", ovvero dell'art. 32 del Regolamento).

Ne discende che, allorquando il titolare del trattamento si risolva ad adottare misure tecniche e organizzative meno costose, le stesse devono essere comunque altrettanto efficaci nel mitigare i rischi che insistono sui dati. Come, infatti, evidenziato dal Garante, "i costi di attuazione non possono essere considerati un elemento che autorizzi il titolare del trattamento ad abbassare il livello di protezione che le misure devono assicurare in maniera adeguata; semmai, essi possono costituire un fattore da tenere in conto nella scelta tra più soluzioni" (provv. 17 luglio 2024, n. 475, doc. web n. 10057648),

Nel caso di specie, l'Ordine non può, pertanto, invocare la limitatezza delle proprie risorse organizzative e finanziarie per giustificare la mancata adozione di misure adeguate a fronteggiare i rischi derivanti dai trattamenti da esso posti in essere. D'altra parte, a seguito della violazione di dati personali in questione, l'Ordine si è determinato a installare un "software tool per la rilevazione di minacce alla sicurezza dei dati" (v. nota del 19 gennaio 2024, pag. 4), avendo, dunque, l'Ente potuto a sostenere il costo economico derivante dall'adozione di tale misura.

I titolari del trattamento sono poi tenuti a considerare i costi di attuazione assieme agli ulteriori fattori contemplati dall'art. 32 del Regolamento, ovvero lo "stato dell'arte", la "natura, […] l'oggetto, [il] contesto e [le] finalità del trattamento", nonché il "rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche" (cfr. art. 25 del Regolamento).

Quanto allo "stato dell'arte", si tratta di "un concetto dinamico che non può essere definito staticamente con riguardo a un determinato momento, bensì dovrebbe essere oggetto di una valutazione continuativa nel contesto dei progressi tecnologici"; esso "impone l'obbligo ai titolari, allorché determinano le misure tecniche e organizzative adeguate, di tenere conto degli attuali progressi compiuti dalla tecnologia disponibile sul mercato", con la conseguenza che "i titolari debbano essere a conoscenza dei progressi tecnologici e rimanere sempre aggiornati sulle opportunità e i rischi per il trattamento, in termini di protezione dei dati, derivanti dalle tecnologie e su come mettere in atto e aggiornare le misure e le garanzie che assicurano un'attuazione efficace dei principi e dei diritti degli interessati tenendo conto dell'evoluzione del panorama

tecnologico” (“Linee guida 4/2019 sull’articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita”, cit., parr. 18-20).

Tenuto conto, come sopra detto, dell’aggravarsi del rischio cibernetico negli ultimi anni, l’adozione dei menzionati sistemi automatizzati di alert deve considerarsi, nel contesto di trattamento in questione, una misura adeguata allo stato dell’arte della tecnologia e all’attuale scenario di rischio. Le “Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD”, adottate dal Comitato europeo per la protezione dei dati il 28 marzo 2023 (di seguito, le “Linee guida sulla notifica”), evidenziano, infatti, che “la capacità di individuare, trattare e segnalare tempestivamente una violazione deve essere considerata un aspetto essenziale” delle misure tecniche e organizzative che il titolare e il responsabile del trattamento devono mettere in atto, ai sensi dell’art. 32 del Regolamento, per garantire un livello adeguato di sicurezza dei dati personali (par. 41; cfr. provv. 17 luglio 2024, n. 444, doc. web n. 10057610).

In merito alla “natura, [all’] oggetto, [al] contesto e [alle] finalità del trattamento”, l’Ordine avrebbe dovuto debitamente tenere in considerazione la circostanza che, nell’ambito della trattazione dei procedimenti disciplinari, esso può trattare dati personali di soggetti vulnerabili (pazienti; minori), anche relativi a categorie particolari di dati oppure a condanne penali o reati.

Il par. 2 dell’art. 32 del Regolamento precisa poi che, nel valutare l’adeguato livello di sicurezza, si deve tener conto, in special modo, dei rischi presentati dal trattamento, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso non autorizzato, in modo accidentale o illegale, ai dati personali. Anche a tal riguardo, l’Ordine, ai fini dell’individuazione delle necessarie misure tecniche e organizzative, avrebbe dovuto considerare gli elevati rischi per gli interessati che sarebbero potuti conseguire da un eventuale divulgazione delle predette delicate informazioni, in termini di conseguenze sulle relazioni economiche e sociali degli interessati, con particolare riguardo all’ambito familiare, scolastico o lavorativo, come, peraltro, emerge dalla segnalazione e dai reclami pervenuti.

Alla luce delle considerazioni che precedono, deve concludersi che la mancata adozione da parte dell’Ordine delle predette misure tecniche e organizzative configura una violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento.

3.3 La mancata adozione di misure adeguate a garantire la sicurezza dei sistemi di trattamento.

A parziale rettifica e chiarimento delle dichiarazioni rese nel corso dell’istruttoria, l’Ordine, integrando le dichiarazioni rese nel corso dell’audizione, ha affermato che "l'accesso ai sistemi informatici dell'Ordine è avvenuto a causa di una vulnerabilità di un punto di accesso RDP dell'infrastruttura dell'Ordine, sebbene gli attaccanti abbiano tentato di utilizzare credenziali che, con ogni probabilità, erano già in loro possesso (verosimilmente tramite il dark web) o generate attraverso un attacco di tipo brute force”, precisando che “le credenziali sottratte non consentivano di accedere alla rete dell'Ordine (ovvero al sistema RDP esposto)”. Pertanto, ad avviso dello stesso, “anche qualora l'Ordine avesse adottato soluzioni di autenticazione a più fattori, questo non avrebbe evitato il verificarsi della violazione di dati personali”.

Richiamato quanto evidenziato al precedente par. 3.2 in relazione a quanto previsto dagli artt. 24 e 32 del Regolamento, con particolare riguardo all’impossibilità di invocare i costi di attuazione per giustificare la mancata adozione delle necessarie misure tecniche a protezione dei dati, nonché tenuto conto che l’adeguatezza delle misure attuate dal titolare del trattamento deve essere valutata in concreto, in ragione dei diversi criteri previsti da tali articoli e delle esigenze di protezione dei dati specificamente inerenti al trattamento nonché ai rischi indotti da quest’ultimo (v. Corte di Giustizia dell’Unione europea, sentenze C687/21, MediaMarktSaturn, del 25 gennaio 2024, par. 38, e C340/21, Natsionalna agentsiaza prihodite, parr. da 30 a 32), deve osservarsi che

i trattamenti effettuati dall'Ordine nel contesto in esame avrebbero richiesto l'adozione di misure tecniche e organizzative adeguate allo stato dell'arte, al fine di assicurare la riservatezza dei dati personali dei soggetti interessati. Ciò, come sopra detto, anche alla luce delle finalità dei trattamenti (effettuati anche nell'ambito di procedimenti disciplinari), dell'elevato numero degli interessati, della natura delicata dei dati personali trattati (appartenenti anche a categorie particolari e relativi a condanne penali e reati), nonché dei possibili rischi per i diritti e le libertà degli interessati, tra cui anche soggetti vulnerabili (pazienti, minori, lavoratori).

Dall'attività istruttoria è, invece, emerso che l'Ordine non aveva adottato misure adeguate a garantire la sicurezza dei sistemi di trattamento. In particolare, l'Ordine non aveva adottato un sistema di autenticazione a più fattori (MFA), che avrebbe potuto impedire l'accesso non autorizzato ai sistemi anche a fronte della compromissione delle credenziali di autenticazione. Soltanto a seguito dell'incidente, l'Ordine ha, infatti, ritenuto necessario "l'adozione di un sistema di autenticazione a più fattori (MFA)" (v. notifica del 20 novembre 2023, sez. H, punto 2 e nota del 19 gennaio 2024, pagg. 4 - 5).

Deve poi osservarsi che, ancorché l'Ordine abbia dichiarato che le credenziali in passato esfiltrate e presenti nel dark web non siano state utilizzate ai fini dell'attacco in questione, in quanto relative alla posta elettronica, tali credenziali non erano state comunque adeguatamente protette mediante cifratura, non potendosi, peraltro, escludere che gli attaccanti abbiano provato a utilizzare le medesime credenziali o altre credenziali simili per perpetrare l'attacco.

Da ultimo, dalle dichiarazioni rese dall'Ordine emerge che il server vettore d'ingresso dell'attacco risultava dotato di un sistema operativo obsoleto (XX), le cui vulnerabilità (servizio RDP esposto su porta di default) sono state sfruttate dall'attaccante per penetrare nell'infrastruttura dell'Ente.

Alla luce delle considerazioni che precedono, la mancata adozione, al momento della violazione, di misure adeguate a garantire la sicurezza dei sistemi di trattamento configura una violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell'Ufficio e si rileva la molteplice violazione, da parte dell'Ordine, degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento.

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave, relativa all'art. 5, par. 1, lett. f), del Regolamento, è soggetta alla sanzione prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, atteso che, come sopra evidenziato, l'Ordine ha dichiarato di aver adottato le opportune misure tecniche e organizzative per prevenire simili eventi in futuro, non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento.

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

ancorché l'Ordine non avesse adottato sistemi di alert in tempo reale per l'identificazione tempestiva di eventuali anomalie, lo stesso aveva quantomeno implementato un firewall in grado di rilevare i log e i tentativi di connessione RDP (Remote Desktop Protocol) dall'esterno, inclusi eventuali tentativi di accesso indebito alla rete, affidando a taluni propri dipendenti il controllo periodico degli stessi (cfr. art. 83, par. 2, lett. a), del Regolamento);

l'esfiltrazione dei dati è avvenuta in maniera progressiva, ovvero generando quantità di traffico di dimensioni tali da non generare sospetti, in orario notturno e in giorni festivi, senza mai superare la soglia di traffico media, che evidentemente, per motivi non noti, era conosciuta dagli attaccanti (cfr. art. 83, par. 2, lett. a), del Regolamento);

la violazione non ha compromesso la disponibilità e l'integrità dei dati personali trattati dall'Ordine (cfr. art. 83, par. 2, lett. a), del Regolamento);

la violazione ha, tuttavia, riguardato un elevato numero di dati personali ("circa 15.000 registrazioni"; "6,9GB"), fra cui dati anagrafici, di contatto, di pagamento, relativi a documenti d'identità/riconoscimento, appartenenti a categorie particolari (ovvero dati che rivelano l'origine etnica, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la vita sessuale o l'orientamento sessuale, lo stato di salute), relativi a condanne penali e reati, e coperti dal segreto professionale, con la conseguenza che i numerosi interessati a cui gli stessi si riferiscono ("3.000", di cui una parte coinvolti a vario titolo in 159 procedimenti disciplinari), tra cui anche soggetti vulnerabili (minori, pazienti, lavoratori), sono stati esposti a potenziali rischi di discriminazione, furto d'identità, frodi, rischi reputazionali e altri pregiudizi nella sfera economica e sociale (art. 83, par. 2, lett. a) e g), del Regolamento);

tenuto conto dei predetti rischi per i diritti e le libertà degli interessati, nonché considerati, da un parte, l'attuale elevato livello di rischio cibernetico e, dall'altro, lo stato dell'arte nel settore della sicurezza informatica, la condotta dell'Ordine, che consiste nell'aver omesso di adottare le richiamate misure tecniche e organizzative a presidio dei dati, deve considerarsi negligente, fermo restando che l'esfiltrazione e la diffusione dei dati sono comunque imputabili a un comportamento doloso posto in essere da un'organizzazione criminale

("NoEscape"), mediante un ransomware diffusosi in tempi relativamente recenti (art. 83, par. 2, lett. b), del Regolamento);

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento, ancorché dotato di una limitata struttura organizzativa (tredici dipendenti) è un Ente pubblico di rilevanza regionale, che gestisce numerosi iscritti (25.499; fonte www.opl.it), si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

la violazione, che, in ragione della natura dei dati coinvolti e delle categorie di interessati cui gli stessi si riferiscono, si connota di particolare gravità, ha avuto luogo per effetto dell'omessa adozione di adeguate misure tecniche e organizzative, rispetto alla quale l'Ordine ha un elevato grado di responsabilità (art. 83, par. 2, lett. d), del Regolamento);

l'Ordine ha notificato al Garante la violazione dei dati personali ai sensi dell'art. 33 del Regolamento e ha offerto una buona cooperazione con l'Autorità nel corso dell'istruttoria, avendo, peraltro, provveduto ad adottare nuove misure tecniche e organizzative volte a rafforzare la sicurezza dei trattamenti e a prevenire eventuali simili attacchi informatici per il futuro (art. 83, par. 2, lett. f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 30.000 (trentamila) per la molteplice violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò, come sopra evidenziato, in considerazione del contesto di trattamento particolarmente delicato in cui la violazione si è verificata, sia per la natura dei dati personali oggetto di trattamento sia per le caratteristiche soggettive degli interessati, tra cui figurano anche soggetti vulnerabili.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, che il trattamento è avvenuto in violazione degli artt. 5, par. 1, lett. f), e 32, par. 1, del Regolamento, nei termini di cui in motivazione;

ORDINA

all'Ordine degli Psicologi della Regione Lombardia, in persona del legale rappresentante pro-tempore, con sede legale in Corso Buenos Aires, 75 - 20124 Milano (MI), C.F. 97134770151, di pagare la somma di euro 30.000 (trentamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la

controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto Ordine, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di 30.000 (trentamila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 29 aprile 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE REGGENTE
Filippi