DELIBERAZIONE 25 MARZO 2025
106/2025/S/COM

IRROGAZIONE DI UNA SANZIONE AMMINISTRATIVA PECUNIARIA PER VIOLAZIONE DI DISPOSIZIONI IN MATERIA DI FUNZIONAMENTO DEL SISTEMA INFORMATIVO INTEGRATO

L'AUTORITÀ DI REGOLAZIONE PER ENERGIA RETI E AMBIENTE

Nella 1333ª riunione del 25 marzo 2025

VISTI:

- la direttiva 2009/73/CE del Parlamento Europeo e del Consiglio del 13 luglio 2009 relativa a norme comuni per il mercato interno del gas naturale;
- la direttiva (UE) 2019/944 del Parlamento Europeo e del Consiglio del 5 giugno 2019 relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE;
- la direttiva (UE) 2024/1788 del Parlamento europeo e del Consiglio del 13 giugno 2024 (di seguito: direttiva 2024/1788);
- la legge 24 novembre 1981, n. 689 (di seguito: legge 689/81);
- la legge 14 novembre 1995, n. 481 e s.m.i. e, in particolare, l'articolo 2, comma 20, lettera c) (di seguito: legge 481/95);
- il decreto legislativo 16 marzo 1999, n. 79;
- il decreto legislativo 23 maggio 2000, n. 164;
- il decreto del Presidente della Repubblica 9 maggio 2001, n. 244;
- l'articolo 11 *bis*, del decreto-legge 14 marzo 2005, n. 35, introdotto dalla legge di conversione 14 maggio 2005, n. 80, come modificato dal decreto-legge 9 dicembre 2023, n. 181;
- la legge 23 luglio 2009, n. 99;
- il decreto-legge 8 luglio 2010, n. 105, recante "Misure urgenti in materia di energia" convertito con legge 13 agosto 2010, n. 129 (di seguito: decreto-legge 105/10);
- il decreto legislativo 1 giugno 2011, n. 93 e s.m.i. (di seguito decreto legislativo 93/11);
- la deliberazione dell'Autorità di Regolazione per Energia Reti e Ambiente (di seguito: Autorità) 17 novembre 2010, ARG/com 201/2010 (di seguito: deliberazione ARG/com 201/10), recante le "Direttive per lo Sviluppo del Sistema Informativo Integrato per la gestione dei rapporti fra i diversi operatori dei mercati liberalizzati" e il relativo Allegato A come successivamente modificato e integrato (di seguito: Allegato A alla deliberazione ARG/com 201/10);

- la deliberazione dell'Autorità 8 marzo 2012, 79/2012/R/com di "Approvazione del regolamento di funzionamento del Sistema Informativo Integrato" (di seguito: deliberazione 79/2012/R/com);
- la deliberazione dell'Autorità 10 novembre 2020, 455/2020/R/com (di seguito: deliberazione 455/2020/R/com), recante "Approvazione del Regolamento di funzionamento del Sistema Informativo Integrato aggiornato";
- l'Allegato A alla deliberazione dell'Autorità 19 dicembre 2023, 598/2023/E/com recante "Modifiche al regolamento per la disciplina dei procedimenti sanzionatori e delle modalità procedurali per la valutazione degli impegni" (di seguito: Regolamento Sanzioni);
- il Regolamento del SII *pro tempore* vigente (di seguito: Regolamento del SII o anche Regolamento) e i relativi allegati, e in particolare l'allegato A recante "Modello tecnologico del SII" e l'Allegato C recante "Regole e misure di sicurezza";
- le "Specifiche tecniche del Portale *WEB*" del SII del 4 dicembre 2013;
- la determinazione del Direttore della Direzione Sanzioni e Impegni dell'Autorità del 17 aprile 2024, DSAI/13/2024/com (di seguito: determinazione DSAI/13/2024/com).

FATTO:

1. Con nota 25 ottobre 2023 (acquisita con prot. Autorità 66961), successivamente integrata con nota 21 marzo 2024 (acquisita con prot. Autorità 21089), Acquirente Unico S.p.A. in qualità di Gestore del Sistema Informativo Integrato (di seguito anche Gestore del SII o AU) ha segnalato all'Autorità la potenziale violazione del Regolamento del SII da parte di alcuni Utenti, tra cui Axpo Italia S.p.A. (di seguito Axpo Italia, Axpo o Società), che risultavano avere divulgato le proprie credenziali di accesso al SII a persone fisiche diverse dall'utente finale cui erano intestate in via esclusiva e/o averle utilizzate tramite c.d. BOTNET.
2. Segnatamente, in data 17 luglio 2023 AU disabilitava un'utenza di Axpo Italia a causa del rilevamento di un'attività sospetta: con le credenziali di un *utente finale* (ossia, ai sensi dell'art. 1, comma 1.1, del Regolamento del SII, di una "*persona fisica autorizzata dall'Utente ad operare con il SII*") venivano effettuati, in ventiquattro ore, oltre mille tentativi di accesso al SII (circa 1700), nonostante il Portale del SII fosse in manutenzione e pubblicasse una pagina *web* statica che recava il messaggio di indisponibilità dei servizi. In data 19 luglio 2023 la Società chiedeva lo sblocco della predetta utenza aprendo un *ticket*, al quale l'*Help Desk* di AU rispondeva domandando chiarimenti in merito a quanto rilevato e, in particolare, se l'utente in questione utilizzasse *software* o piattaforme automatiche robotiche collegate ai servizi del SII. Nella stessa data Axpo Italia confermava l'uso di un *software* automatizzato per l'accesso al SII, dichiarando di usare "*un tool automatizzato di accesso al portale che scarica alcune prestazioni dal massivo come le VPU (...) e utilizza l'utenza (...) che al momento è bloccata*". Il 28 luglio 2023 Axpo Italia reiterava la richiesta di sblocco dell'utenza, affermando che le attività rilevate da AU non si configuravano come possibili attacchi esterni o uso delle credenziali da parte di soggetti terzi. Il 3 agosto 2023 l'*Help Desk* di AU comunicava che, tramite

Procedura di *Reset,* sarebbe stata ripristinata la *UserID* bloccata e che la stessa sarebbe stata costantemente monitorata.

3. Dagli approfondimenti svolti dal Gestore del SII in esito alla interlocuzione con Axpo Italia, veniva rilevato l'utilizzo della predetta *UserID*, relativa a persona fisica e strettamente personale, tramite BOTNET, dunque, in contrasto con le prescrizioni del Regolamento del SII; al contempo, AU dava atto che alla data del 22 febbraio 2024 non risultavano ulteriori condotte anomale (relazione allegata alla nota di AU acquisita con prot. Autorità 21089 del 21 marzo 2024).
4. Pertanto, in esito all'esame della documentazione trasmessa, con determinazione DSAI/13/2024/com l'Autorità ha avviato nei confronti di Axpo Italia un procedimento sanzionatorio ai sensi dell'articolo 2, comma 20, lettera c), della legge 481/95 per l'accertamento della violazione di alcune disposizioni in materia di funzionamento del SII.
5. In particolare, con la determinazione di avvio del presente procedimento è stata contestata alla Società la violazione dell'articolo 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10 e degli articoli 6, comma 1, lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento.
6. Il 23 aprile 2024 la Società ha presentato istanza di accesso ai documenti (acquisita con prot. Autorità 29866), accolta dal Responsabile del procedimento in data 8 maggio 2024 (prot. Autorità 32766), previa comunicazione ai sensi dell'articolo 3 del d.P.R. 184/2006 e dell'articolo 17 dell'Allegato A alla deliberazione 412/2021/A ad Acquirente Unico S.p.A. (con prot. Autorità 30073 del 24 aprile 2024).
7. In data 9 maggio 2024 la Società ha presentato una richiesta di proroga (acquisita con prot. Autorità 32925) del termine per la presentazione di impegni di cui all'art. 20 del Regolamento Sanzioni, non accolta dal Responsabile del procedimento in ragione della natura espressamente decadenziale del predetto termine (prot. Autorità 33336 del 13 maggio 2024).
8. Successivamente, con nota del 17 maggio 2024 (acquisita con prot. Autorità 36085) Axpo Italia ha tempestivamente presentato, ai sensi dell'articolo 45, comma 3, del decreto legislativo 93/11 e dell'articolo 20 del Regolamento Sanzioni, una proposta di impegni relativa al procedimento sanzionatorio in oggetto. Tale proposta di impegni è stata dichiarata inammissibile con deliberazione dell'Autorità del 2 luglio 2024, 268/2024/S/com.
9. In data 2 settembre 2024 la Società ha trasmesso una memoria difensiva (acquisita con prot. Autorità 62521 del 3 settembre 2024).
10. Con nota del 22 ottobre 2024 (prot. Autorità 74262) il Responsabile del procedimento ha comunicato le risultanze istruttorie.
11. Con memoria di replica del 6 dicembre 2024 (prot. Autorità 85466) la Società ha replicato alle risultanze istruttorie, ha fornito aggiornamenti in ordine alle proprie condizioni economiche (indicando i dati di ricavo al 30 settembre 2024) e ha trasmesso due pareri elaborati da un consulente di parte, ad integrazione della memoria di replica alle risultanze istruttorie.

12. In data 28 ottobre 2024 la Società ha richiesto di essere sentita in audizione finale innanzi al Collegio (prot. Autorità 75711). L'audizione finale innanzi al Collegio si è svolta il 30 gennaio 2025.

VALUTAZIONE GIURIDICA:

13. Il Sistema Informativo Integrato (di seguito: SII) è stato istituito presso AU con l'articolo 1-bis, primo comma, del decreto-legge 105/10 per sostenere la competitività e la funzionalità delle imprese operanti nei mercati dell'energia elettrica e del gas naturale, ed all'Autorità è stato affidato il compito di emanare i criteri generali per il suo funzionamento. Il SII, basato su una "*banca dati dei punti di prelievo e dei dati identificativi dei clienti finali*", costituisce un'infrastruttura essenziale poiché è la sede esclusiva, che progressivamente sostituisce tutti i precedenti sistemi informatici, ove i diversi operatori dei mercati energetici interagiscono, secondo la regolazione dell'Autorità, per lo svolgimento delle attività della filiera del settore dell'energia e, in particolare, allo scopo di dare esecuzione ai rapporti contrattuali con i clienti finali. La disciplina che definisce i processi, ossia le prestazioni rese attraverso il SII, nonché quella che stabilisce le modalità di funzionamento del SII stesso e che concerne in particolare le modalità di interazione tra il Gestore del SII e i suoi utenti, sono pertanto fondamentali per garantire uno svolgimento dei servizi regolati continuativo, trasparente e sicuro.
14. In attuazione del predetto articolo 1-bis, l'Autorità con la deliberazione ARG/com 201/10 ha dettato le prime direttive per lo sviluppo del SII e, segnatamente con l'Allegato A alla citata deliberazione, recante "*Criteri generali, modello di funzionamento e modello organizzativo del SII*", ha stabilito che:
    - sulla base dei criteri generali ivi indicati, il Gestore del SII, ovvero AU, predispone un Regolamento che disciplini il funzionamento del SII, inclusi i rapporti tra il SII e gli Utenti, le modalità di trattamento dei dati personali e sensibili e i requisiti e le condizioni di accesso al sistema; detto Regolamento deve essere approvato dall'Autorità (articolo 2, commi 6 e 8);
    - AU garantisce la sicurezza, la riservatezza delle informazioni e la loro salvaguardia nel tempo e a tal fine si dota di adeguate procedure per garantire che ogni accesso ai dati contenuti nel SII sia tracciabile e sia univocamente riferibile agli Utenti autorizzati (articolo 5, comma 1);
    - "*ciascun Utente è autonomo nella gestione dei propri sistemi, nella definizione e nella attuazione delle politiche di sicurezza del proprio sistema informativo, fermo restando l'obbligo di rispettare le disposizioni del regolamento di cui al comma 2.6 e in particolare i requisiti minimi di sicurezza previsti*" (articolo 6 comma 1, lettera d).
15. Conformemente alle predette disposizioni, AU ha predisposto il Regolamento del SII e i relativi allegati, che sono stati approvati dall'Autorità con deliberazione 79/2012/R/com e con deliberazione 455/2020/R/com, e sono pubblicati sul sito internet di AU. Quest'ultimo, poi, in attuazione dell'articolo 14 comma 1 punto 2) del citato Regolamento, ha adottato – tra l'altro – le "*Specifiche tecniche del Portale*

WEB" del SII ovvero dell'interfaccia standardizzata per l'interazione sicura, certificata e controllata, tra gli utenti finali e l'infrastruttura centrale del SII. Ai sensi dell'articolo 1 del predetto Regolamento:

- "*Utente*" è il "*soggetto giuridico che partecipa al SII*", come ad esempio le società di vendita e le imprese di distribuzione;
- "*Utente finale*" è "*la persona fisica autorizzata dall'Utente ad operare con il SII*";
- gli "*Strumenti di Comunicazione Evoluta*" (di seguito anche applicazioni o sistemi) sono le componenti standardizzate, previste nel modello tecnologico del SII, per l'interazione tra il sistema informatico dell'Utente e l'infrastruttura centrale.

16. Ai sensi dell'articolo 6 del Regolamento, gli Utenti, in quanto operatori che svolgono attività soggette a regolazione, devono – tra gli altri obblighi – assicurare "*il rispetto delle misure di sicurezza e dei livelli di servizio secondo quanto indicato (...) nell'allegato C (...) del Regolamento*" (articolo 6, comma 1, lettera c, e articolo 15, comma 3), il quale allegato C a sua volta ribadisce che gli Utenti "*sono responsabili (...) del corretto utilizzo del portale web*" e "*sono direttamente responsabili anche nel caso in cui la gestione dei servizi informatici sia affidata a terzi*" (sezioni 1 e 2.1 dell'allegato C). In particolare, ciascun Utente al momento dell'accreditamento presso il SII (articolo 9 comma 1 del Regolamento del SII e paragrafo 5 delle "*Specifiche tecniche del Portale WEB*") deve indicare:
    - il Responsabile del SII, cioè la persona fisica che rappresenta l'Utente nei confronti del SII;
    - il Referente tecnico, cioè la persona fisica a cui è assegnato il compito di sovrintendere alla realizzazione ed al funzionamento delle componenti tecniche necessarie alla corretta gestione dei processi;
    - il Responsabile della sicurezza, cioè la persona fisica a cui è assegnata la responsabilità relativa alla gestione della sicurezza e che "*Gestisce ed è garante delle credenziali di accesso degli utenti finali e dei certificati necessari all'interazione con il SII*".
17. Inoltre, per ciascun Processo (cioè servizio o prestazione) del SII (come *switching*, voltura, *pre-check*, consultazione puntuale o massiva), il Regolamento del SII e le Specifiche tecniche del Portale WEB prevedono che: il Responsabile del SII nomina il referente del Processo, il quale a sua volta nomina e coordina le persone fisiche che per conto dell'Utente sono autorizzate a svolgere le attività operative sul SII (operatori di Processo) tramite accesso via Portale WEB, definendo anche il profilo di abilitazione da associare a ciascuna di esse (articolo 11, comma 3 del Regolamento del SII e paragrafi 5 e 7.2 delle Specifiche tecniche). Tutte le modifiche alle predette informazioni, inclusa la revoca dell'abilitazione alle persone fisiche indicate, devono essere tempestivamente comunicate dall'Utente al Gestore del SII (articolo 11, comma 4 del Regolamento del SII e paragrafi 7.2.1 e 7.2.3 delle Specifiche tecniche). Sulla base dei nominativi comunicati dal Referente del Processo, il Gestore del SII gestisce le autorizzazioni, individuando per ciascuno di essi le modalità di accesso personali corrispondenti al ruolo e al profilo di accesso indicato (quali ad esempio

accesso in sola lettura, lettura e scrittura, annullamento) (articolo 11, comma 6 del Regolamento del SII).

18. Ciascun Utente può operare con il SII anche mediante gli strumenti di comunicazione evoluta previsti dal modello tecnologico di cui all'Allegato A al Regolamento (articoli 8, comma 2, e 10 del Regolamento del SII), cioè la Porta di Comunicazione e il servizio di *Cloud Storage* (paragrafo 3 dell'allegato A), e in questo caso deve effettuare le procedure di qualificazione di cui al successivo articolo 14, finalizzate a verificare, tra l'altro, il rispetto delle misure di sicurezza e dei livelli di servizio di cui al medesimo articolo. Tali misure di sicurezza sono diverse da quelle previste per l'accesso delle persone fisiche tramite Portale WEB.
19. Ai sensi del predetto articolo 14, comma 1, del Regolamento del SII, al fine della corretta ed efficace realizzazione del SII e del successivo funzionamento, il Gestore del SII definisce regole tecniche, specifiche tecniche e linee guida che l'Utente ha l'obbligo di rispettare; segnatamente:
    - "*le regole tecniche per l'accreditamento al SII, contenenti almeno le regole e le misure di sicurezza*" di cui all'allegato C al Regolamento del SII (il cui rispetto è richiamato anche dal successivo articolo 15 comma 3) (punto 1);
    - "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo del Portale WEB del SII*" (punto 2);
    - "*le specifiche tecniche e di sicurezza (…) necessarie all'utilizzo degli strumenti di comunicazione evoluta, comprese le procedure di qualificazione*" (punto 3).
20. La sezione 2.2 dell'Allegato C prevede, tra gli obiettivi di sicurezza del SII, che ogni accesso ai dati contenuti nel SII debba essere tracciabile e univocamente riferibile alle entità *autorizzate*, siano esse utenti finali (cioè persone fisiche) o strumenti di comunicazione evoluta secondo le definizioni di cui al citato articolo 1 del Regolamento del SII. Per tale ragione, l'erogazione e la fruizione di un servizio applicativo del SII richiede che siano *preliminarmente* effettuate operazioni di *identificazione* univoca delle entità (basate su *UserID* per gli utenti finali che accedono tramite Portale WEB e su URI, *Uniform Resource Identifier*, per i sistemi che accedono tramite strumenti di comunicazione evoluta) e di *autenticazione* delle medesime mediante meccanismi anch'essi individuali (password e/o meccanismi di autenticazione forte, cioè il certificato digitale su dispositivo elettronico fisico, ad esempio *smartcard*, o virtuale, ad esempio il *token* virtuale, ed il PIN, per gli utenti finali; certificati digitali "*emessi dalla Autorità di Certificazione (CA) della Infrastruttura a Chiave Pubblica (PKI) del SII o da un Certificatore accreditato secondo la normativa vigente*" per gli strumenti di comunicazione evoluta) (sezione 2.4 e sezioni 3 e 4 dell'allegato C nonché paragrafo 9 delle Specifiche tecniche). Gli Utenti possono disporre di uno o più *account* di accesso (sezione 4 dell'allegato C), ma in ogni caso "*Le credenziali associate agli utenti finali sono strettamente personali, non possono essere cedute a terzi ed il possessore si assume la responsabilità della loro custodia garantendo la confidenzialità delle stesse*" (sezione 2.4.2 dell'allegato C al Regolamento del SII e paragrafo 9.2.7 delle Specifiche tecniche del Portale WEB).

Argomentazioni difensive di Axpo Italia

21. La Società ha svolto un'intensa attività difensiva nell'ambito del procedimento, esercitando tutti i diritti riconosciutile dal Regolamento Sanzioni, tra l'altro trasmettendo, in fase decisoria, una articolata memoria difensiva con la quale ha riorganizzato e ulteriormente sviluppato le proprie difese, allegando altresì due pareri di un consulente tecnico a supporto di alcune delle proprie argomentazioni, poi di nuovo richiamate, insieme ad altre difese, in sede di audizione finale innanzi al Collegio. Per semplicità si segue l'impostazione difensiva prospettata nella memoria di replica alle risultanze istruttorie e poi ancora nell'audizione finale, salvo riprendere – eventualmente nel successivo paragrafo riferito alla valutazione – gli argomenti proposti in fase istruttoria e poi non ripresi in fase decisoria.
22. La Società ha contestato *in radice* la sussistenza stessa degli elementi costitutivi dell'illecito (condotta ed evento).
23. La Società, pur consapevole che "*per l'illecito di pericolo…non occorre la lesione del bene giuridico tutelato*", sostiene anzitutto l'insussistenza dell'evento, poiché "*l'evento giuridico richiesto dalla norma non si [è] verificato (non essendo mai avvenuto…l'accesso al SII) e di conseguenza nessuna violazione può essere contestata ad AXPO. Gli Uffici non hanno infatti prodotto alcuna evidenza per dimostrare un effettivo vulnus del SII, ritenendone addirittura superfluo l'accertamento [vertendosi di un illecito di pericolo]*".
24. Né, sostiene la Società, risulterebbe integrata la condotta illecita, in quanto:
    (i) non vi sarebbe stata alcuna cessione a terzi delle credenziali personali rilasciate all'Utente finale ("*Una volta che il personale Axpo ha avuto accesso all'interfaccia utente del programma Xbot, deve configurare la sua utenza, inserendo le proprie credenziali di accesso (…). Solo in un secondo momento il tool richiedeva di effettuare l'accesso al SII tramite le credenziali personali che AU ha affidato all'Utente. Le credenziali, quindi, non sono mai state cedute a terzi (ad es. consulenti esterni o altri dipendenti dell'Utente diversi dall'Utente finale cui le credenziali sono state assegnate), ma inserite effettivamente da chi è legittimato a farlo*");
    (ii) come già evidenziato, si è registrato solo un tentativo di accesso al SII (rimasto incompiuto a causa di un malfunzionamento dell'infrastruttura informatica);
    (iii) il ricorso al programma XBot per accedere al portale *web* del SII non sarebbe vietato. In particolare, il Regolamento SII individuerebbe gli strumenti di comunicazione evoluta "*ad oggi disponibili (la PdC e il servizio di Cloud Storage)*", senza limitare le modalità attraverso le quali l'Utente finale può collegarsi al SII (manualmente o attraverso altri strumenti quali ad esempio tool automatizzati). A conferma della propria tesi la Società richiama:
    a) l'Allegato C al Regolamento SII che prevede espressamente che ogni accesso "*ai dati contenuti nel SII deve essere […] tracciabile e univocamente riferibile alle entità autorizzate (siano esse utenti finali o applicazioni di sistema)*" e che "*anche Operatori Massivi [cfr. Specifiche tecniche del Portale Web] siano*

autorizzati ad accedere al SII, necessitando a tal fine di tool automatizzati per scaricare dati in modo massivo";

b) la previsione contenuta nell'art. 6, comma 1, lett. d dell'Allegato A alla deliberazione 201/10 ("*ciascun utente è autonomo nella gestione dei propri sistemi, nella definizione e nella attuazione delle politiche di sicurezza del proprio sistema informativo, fermo restando l'obbligo di rispettare le disposizioni del regolamento di cui al comma 2.6 e in particolare i requisiti minimi di sicurezza*") che "*non impedisce il ricorso a strumenti automatizzati per accedere al SII (in particolare laddove, come nel caso di specie, l'accesso sia avvenuto attraverso il portale web), sempreché siano per l'appunto rispettati i requisiti minimi di sicurezza elencati nel citato Allegato C. E ciò considerando …che il tool utilizzato da AXPO non può essere assimilato ad una PdC o al Cloud storage (i.e. gli unici strumenti di comunicazione evoluta attualmente ammessi dall'Allegato A al Regolamento del SII) e di riflesso non dovrebbe sottostare alla procedura di autorizzazione ed autenticazione che il regolamento del SII circoscrive per l'accesso tramite Pdc e Cloud storage... La norma (…) si limita a prescrivere l'utilizzo di un sistema sicuro*".

25. L'Autorità sarebbe incorsa in una contraddizione laddove, da un lato, ha considerato vietato l'uso del programma XBot e, dall'altro, lo ha considerato alla stregua degli altri strumenti di comunicazione evoluta esistenti, richiedendo anche per questo programma – e quindi con estensione analogica *in malam partem* – l'applicazione delle procedure di autorizzazione espressamente stabilite per la PdC e il *Cloud Storage* e, dunque, "*ammettendo che il programma Xbot può essere utilizzato – e quindi non è di per sé vietato – purché rispetti i medesimi requisiti formali di autorizzazione previsti per PdC e Cloud Storage*". In ogni caso, la Società ritiene che la condotta posta in essere sarebbe inidonea a ledere l'interesse giuridico tutelato dal Regolamento SII.
26. A tal riguardo, Axpo Italia ritiene di aver fornito evidenze circa il rispetto di tutti i requisiti di sicurezza richiesti, così da escludere che il ricorso, nel caso di specie, al programma XBot abbia messo a rischio la sicurezza del Sistema e che tale strumento, in generale, sia in sé idoneo a determinare un *vulnus* alla sicurezza del SII. L'Autorità, peraltro, secondo la Società non avrebbe smentito o confutato tali evidenze nella comunicazione delle risultanze istruttorie, ma si sarebbe limitata a desumere "*una intrinseca pericolosità*" del programma XBot, senza svolgere alcun approfondimento tecnico per analizzarne natura, modalità operative e differenze che intercorrono tra le diverse modalità di accesso e per capire, quindi, se effettivamente sussistono elementi di rischio per la sicurezza legati al suo utilizzo.
27. La Società ribadisce, a tal proposito, che l'infrastruttura Axpo – sulla quale insiste il tool XBot – è stata valutata dal SII stesso "*come rispondente agli standard richiesti in termini di monitoring, penetration test, access control e sicurezza durante la procedura di qualificazione del processo di scaricamento dati dal Cloud SII*", che il suo utilizzo rispetta i criteri di identificazione e autenticazione dei fruitori del SII, garantendone la tracciabilità in ogni fase, che le informazioni ivi desunte non

vengono salvate su *cloud* o altri *data base* esterni alla Società ed infine che il suo utilizzo consente unicamente lo scarico dei documenti e dati relativi a Axpo stessa.

28. Axpo precisa, quindi, i vantaggi derivanti a suo avviso dall'utilizzo di XBot, che – come già indicato nella memoria istruttoria – permetterebbe all'utente finale di svolgere in maniera più efficiente le attività all'interno del SII, di svolgere in modo automatico alcuni processi non implementati tramite PdC ("*non è possibile accedere tramite PdC per il processo di VPU o per consultare puntualmente il RCU, Registro Centrale Ufficiale*") e di evitare "errori tipicamente umani", costituendo così un miglioramento in termini di sicurezza e non un rischio per la stessa.
29. Ai fini della quantificazione dell'eventuale sanzione, la Società chiede che vengano considerate favorevolmente le seguenti circostanze: (i) la condotta, per le ragioni sopra già richiamate, non si sarebbe neppure consumata, essendosi verificato solo un tentativo (rimasto incompiuto) di accesso al SII, reiterato per effetto del malfunzionamento del sistema stesso; (ii) la condotta avrebbe avuto carattere episodico e sarebbe stata di durata minima, come riconosciuto in sede di comunicazione delle risultanze istruttorie ove si è fatto riferimento alle dichiarazioni rese da AU nella relazione del 22 febbraio 2024 che non rilevava ulteriori anomalie; (iii) la Società ha spontaneamente rinunciato, prima dell'avvio del procedimento, ad utilizzare il programma XBot, in tal modo, a suo avviso, non solo attenuando le conseguenze della violazione, ma eliminando *in radice* il presupposto per il loro protrarsi nel tempo (si tratterebbe di circostanze che dovrebbero essere autonomamente valutate in sede di quantificazione della sanzione, sebbene le stesse non siano state valutate positivamente ai fini dell'ammissibilità degli impegni, avendo le due valutazioni finalità diverse); (iv) qualora l'Autorità ravvisasse la colpevolezza dell'agente, essa sarebbe di grado minimo, considerata la convinzione di Axpo di agire legittimamente (convinzione che la Società ritiene abbia fondamento nella lettera delle disposizioni regolatorie); (v) la condotta non avrebbe avuto alcun effetto pregiudizievole sul mercato, sugli utenti, sui clienti finali o sull'azione amministrativa dell'Autorità e la Società non avrebbe tratto indebiti vantaggi dalla violazione (dette circostanze, a parere della Società e contrariamente a quanto sostenuto nella comunicazione delle risultanze istruttorie, devono essere prese in considerazione ai fini di una riduzione della sanzione, ciò in coerenza con l'art. 31, comma 1, lett. b) del Regolamento Sanzioni che valorizza circostanze concrete che connotano la portata, la diffusione e le concrete modalità operative della condotta); (vi) la violazione contestata ad Axpo sarebbe meno grave di quella sanzionata con la deliberazione 479/2024/S/com, adottata nei confronti di altro operatore, e pertanto sarebbe meritevole di un trattamento sanzionatorio più favorevole, non ravvisandosi nel caso di specie (e a differenza dell'altro caso) una cessione delle credenziali a terzi e non avendo Axpo effettuato l'accesso al SII, ma avendolo solo tentato.
30. In sede di audizione finale, la Società – richiamate le difese già svolte, anche sotto il profilo della quantificazione della sanzione – ha ribadito la propria posizione, sostenendo che la normativa di settore non prevede alcun divieto esplicito di collegarsi al portale *web* tramite un *software* come quello da essa utilizzato. Più precisamente, ha evidenziato che l'art. 6, comma 1, lettera d, dell'allegato A alla

deliberazione ARG/com 201/10 stabilisce espressamente che i sistemi impiegati devono essere compatibili con i requisiti minimi di sicurezza e che, pertanto, una volta accertata la conformità del *software* ai principi di sicurezza, nulla osterebbe a che l'accesso al portale *web* avvenga, non solo manualmente, ma anche attraverso un *software* di questo tipo. La Società ha poi ribadito che il processo di autorizzazione e autenticazione previsti dalla Regolazione per la Porta di Comunicazione e per il servizio di *Cloud Storage* non sono altresì richiesti per collegarsi al portale *web* tramite BOTNET. Infine, la Società ha nuovamente evidenziato che la condotta illecita non si sarebbe comunque integrata non essendosi materialmente verificato l'accesso al SII, poiché il sistema informativo era bloccato, in manutenzione, nel momento in cui l'Utente finale (persona fisica) si è collegato con il BOTNET.

31. Con riferimento alla condotta consistente nella cessione delle credenziali, la Società, in sede di audizione finale innanzi al Collegio, ha nuovamente negato che vi sia stata alcuna cessione a terzi delle credenziali rilasciate all'Utente finale (persona fisica dipendente di Axpo).

Le valutazioni delle argomentazioni difensive di Axpo Italia

32. La Società ha ammesso di aver utilizzato credenziali assegnate ad un utente finale persona fisica tramite uno strumento di comunicazione evoluta (non autorizzato) per accedere al Portale *web* del SII.
33. Le argomentazioni svolte dalla Società nel corso del procedimento sono prive di pregio.
34. Anzitutto, sotto il profilo della struttura, l'illecito oggetto di contestazione è un illecito di pericolo e dunque, ai fini della sua integrazione, non rileva in alcun modo la circostanza che dall'utilizzo delle credenziali personali assegnate ad un utente finale persona fisica per accedere tramite BOTNET al Portale SII non sia derivato in concreto un pregiudizio alla sicurezza dei dati del SII e alla struttura informatica (né può rilevare, come si vedrà oltre, che il tentativo di accesso rilevato il 17 luglio 2023 non sia andato a buon fine a causa dei lavori di manutenzione del SII).
35. Né corrisponde al vero l'affermazione secondo la quale non risulterebbe integrata la condotta oggetto di contestazione. Vero è che, in base agli elementi acquisiti al procedimento nella fase istruttoria, non risulta accertata la cessione di credenziali a terzi, persone fisiche e, tuttavia, risulta certamente integrata la diversa e autonoma condotta consistente nell'aver la Società utilizzato credenziali assegnate ad una persona fisica per accedere al Portale *web* del SII tramite un BOTNET, condotta che la Società ha pacificamente ammesso.
    In senso contrario, a nulla vale il richiamo al fatto che i tentativi di accesso al SII rilevati in data 17 luglio 2023 non siano andati a buon fine a causa dei lavori di manutenzione dell'infrastruttura informatica del SII, in quanto la Società ha ammesso di utilizzare normalmente il programma XBot per accedere al SII dal portale *web* (cfr. *supra* punto 24, lett. i.) e non di averlo fatto solo nella giornata del 17 luglio 2023.

36. Priva di pregio è anche l'argomentazione secondo la quale non sussisterebbe nella regolazione un "*divieto di utilizzo del programma Xbot*" per accedere al SII dal portale *web*. In particolare, non trova fondamento né nella lettera delle disposizioni regolatorie, né nella loro *ratio* l'affermazione secondo la quale il Regolamento SII individuerebbe gli strumenti di comunicazione evoluta "*ad oggi disponibili (la PdC e il servizio di Cloud storage)*" senza con ciò limitare le modalità attraverso le quali l'Utente finale può collegarsi al SII e, quindi, senza vietare espressamente l'uso del programma XBot dal portale *web*.
37. Nella consapevolezza che una materia soggetta a rapida evoluzione tecnologica come quella dei sistemi informatici non può essere regolata per il tramite di divieti di utilizzo di particolari strumenti, il Regolamento SII subordina a precisi requisiti di sicurezza posti dal Gestore del SII l'interazione tra il sistema informatico dell'Utente e l'infrastruttura centrale (collaborazione "*Application to Application*"), definendo appunto gli strumenti di comunicazione evoluta come "le componenti *standardizzate*, *previste nel modello tecnologico del SII*, per l'interazione tra il *sistema informatico dell'Utente* e *l'infrastruttura centrale*" (art. 1.1). Gli strumenti di comunicazione evoluti sono una delle quattro "*componenti concettuali*" sulle quali si basa il "*modello tecnologico del SII*" definito dall'Allegato A al Regolamento SII, rappresentando, appunto, una *interfaccia standardizzata per la comunicazione* tra il dominio di responsabilità degli Utenti ed il SII. Il paragrafo 3 dell'Allegato A al Regolamento SII espressamente prevede che "*le interfacce disponibili [per l'interazione tra il sistema informatico dell'Utente e l'infrastruttura centrale] sono la porta di comunicazione, che garantisce l'interazione tra le applicazioni appartenenti a domini diversi mediante l'uso di servizi web [e] il servizio di Cloud Storage, che garantisce lo scambio di file tra domini diversi mediante l'uso di servizi Cloud*". Inoltre, la sezione 3.1 dell'Allegato C al Regolamento SII prevede che "*Ciascun Utente per aderire al SII mediante una collaborazione di tipo Application To Application* deve *dotarsi di una PdC, conforme alle specifiche di cui all'Art.14.1.3 del Regolamento*".
38. Dunque, risulta anzitutto priva di pregio la prospettazione svolta da Axpo (molto chiaramente in fase di audizione), secondo la quale – premesso e riconosciuto che l'accesso al SII avviene con due canali ben distinti, portale e strumenti di comunicazione evoluta – la Società, con il programma XBot, non intendeva utilizzare il canale di accesso degli strumenti di comunicazione evoluta, ma deliberatamente il diverso canale del portale *web*, per il quale la regolazione non vieterebbe l'uso di un *software*. La prospettazione contrasta, infatti, con una basilare regola di sicurezza dei sistemi informatici che, circoscrivendo l'accesso ad un portale *web* alle sole persone fisiche, vuole evitare i più alti rischi connessi alla comunicazione non controllata tra diversi sistemi informatici (si pensi al rischio dell'attacco DDoS, *distributed denial-of-service*, consistente nel generare flussi contemporanei di dati in entrata di dimensioni tali da sovraccaricare un portale internet fino ad esaurirne le risorse e impedirne così il funzionamento).
    Anche per tale ragione il Regolamento del SII, il relativo allegato C e le Specifiche tecniche del Portale WEB:

- distinguono tra le *entità* che accedono al SII: persone fisiche (utenti finali), da un lato, e sistemi, dall'altro (questi ultimi richiedendo una "*collaborazione di tipo Application To Application*" per la quale sono fissati precisi requisiti in apposite specifiche tecniche);
- dispongono che tramite portale *web* accedano unicamente gli utenti finali persone fisiche (e non dunque i sistemi);
- prevedono la definizione di regole di sicurezza diverse per l'accesso e utilizzo del portale *web* e degli strumenti di comunicazione evoluta (evidentemente più incisive per i secondi);
- escludono quindi *in radice* che un sistema – quale è il programma XBot – possa interagire con un altro sistema, quale è quello del SII, per il tramite del portale *web*, attraverso l'uso di credenziali personali rilasciate dal Gestore del SII ad una persona fisica, senza sottostare ai requisiti necessari per la collaborazione *Application to Application*.

39. Priva di pregio è altresì l'affermazione secondo la quale il Regolamento SII individuerebbe gli strumenti di comunicazione evoluta "*ad oggi disponibili (la PdC e il servizio di Cloud storage)*" senza con ciò limitare le modalità attraverso le quali l'Utente finale può collegarsi al SII e, quindi, senza vietare espressamente l'uso del programma XBot dal portale *web*. È da escludersi infatti che possano ammettersi ad interfacciarsi con il SII strumenti di comunicazione evoluta diversi da quelli su menzionati in quanto: a) per espressa previsione regolamentare, le interfacce disponibili "*sono*", appunto, la PdC e il *Cloud storage* e non altre; b) l'indispensabile autonomia operativa di ciascun Utente all'interno del proprio dominio di responsabilità è espressamente garantita nel modello tecnologico del SII proprio individuando, quali strumenti di comunicazione evoluti, la PdC e il *Cloud storage* (cfr. primo e terzo capoverso del paragrafo 3 dell'Allegato A al Regolamento SII) e non altri, in quanto solo questi strumenti sottostanno in modo certo ai parametri di comunicazione fissati dal Gestore del SII, consentendo una comunicazione sì evoluta, ma controllata, e ciò a garanzia del sistema.
40. La Società fornisce quindi una lettura del tutto fallace della previsione contenuta nell'art. 6, comma 1, lett. d) dell'Allegato A alla deliberazione 201/10 secondo la quale "*ciascun utente è autonomo nella gestione dei propri sistemi, nella definizione e nella attuazione delle politiche di sicurezza del proprio sistema informativo, fermo restando l'obbligo di rispettare le disposizioni del regolamento di cui al comma 2.6 e in particolare i requisiti minimi di sicurezza*". La citata disposizione, lungi dal consentire all'Utente di interfacciarsi al SII utilizzando qualsivoglia strumento tecnicamente capace di raggiungere lo scopo, prevede un limite all'autonomia degli Utenti nella gestione dei propri sistemi informativi, costituito proprio dal rispetto dei requisiti minimi di sicurezza. Detti requisiti sono puntualmente indicati nell'Allegato C del Regolamento SII. Rileva, in particolare, il par. 2.4 a mente del quale:
"*l'erogazione e la fruizione di un servizio applicativo richiede che siano effettuate operazioni di* identificazione *univoca delle* entità *(*sistemi *e* utenti finali*) che partecipano, in modo diretto o indiretto (attraverso sistemi intermediari) e con*

ruoli diversi, allo scambio di messaggi, alla erogazione ed alla fruizione dei servizi.
Le regole di Identificazione si basano su UserID per gli utenti finali e su URI per i Sistemi.
(…).
I meccanismi di autenticazione *dipendono dalla tipologia delle* entità *che operano nel SII (*sistemi *e* utenti finali*).*
I meccanismi di autenticazione che riguardano gli utenti finali si basano su UserID e Password.
Le credenziali associate agli utenti finali sono strettamente personali (…).
I meccanismi di autenticazione riguardanti le PdC (per le funzioni di diagnostica, comandi e configurazione della porta) e le funzionalità di autenticazione relative ai Cloud Client devono essere implementati attraverso i protocolli TLS"

Dunque, la prima regola di sicurezza è che *le entità* (persone fisiche o sistemi) che si interfacciano con SII vengano identificate e autenticate, cioè siano riconoscibili dal Sistema Informativo Integrato in modo univoco. In altre parole, ciascun sistema (quale è l'XBot utilizzato da Axpo), così come ciascuna persona fisica, può avere accesso al SII solo se riconosciuto per quello che è, cioè "quel" sistema (o "quella" persona fisica).

41. La previsione, pure richiamata dalla Società nelle proprie difese, secondo la quale "*ogni accesso ai dati contenuti nel SII deve essere tracciabile e univocamente riferibile alle entità* autorizzate *(siano esse utenti finali o applicazioni di sistema)*" presuppone proprio che al SII accedano appunto solo entità *autorizzate,* nel senso già indicato al punto precedente e, ancor più specificamente, al punto 17.
42. Nel caso di specie, è stata quindi violata una primaria regola di sicurezza in quanto un sistema (l'XBot) si è interfacciato al SII, invece che per il tramite della Porta di Comunicazione, come previsto dalle disposizioni sopra richiamate, per il tramite del portale *web*, attraverso il meccanismo di autenticazione proprio delle persone fisiche (utenti finali), ossia attraverso le credenziali strettamente personali associate ad una persona fisica. In tal modo, un BOTNET ha operato su un canale (il portale *web*) destinato a persone fisiche, con performance però "evolute" tipiche dei sistemi automatici, ma senza alcuna possibilità di controllo da parte del Gestore.
43. Nella comunicazione delle risultanze istruttorie non si ravvisa dunque alcuna contraddittorietà: il responsabile del procedimento ha correttamente ritenuto che l'utilizzo da parte di un BOTNET di credenziali strettamente personali per l'accesso al SII per il tramite del portale *web* fosse in contrasto con il Regolamento SII e, allo stesso tempo, ha osservato che il BOTNET può ben accedere al SII, ma con altre modalità, ossia per il tramite della Porta di Comunicazione, soggetta a tutti i requisiti di sicurezza di cui si è detto sopra (cfr., Sezioni 2.2 e 2.4 e dell'allegato C al Regolamento del SII).
44. Quanto all'asserita "*insussistenza di idoneità della condotta a ledere l'interesse giuridico tutelato dal Regolamento SII*", anzitutto si evidenzia che nella documentazione tecnica trasmessa dalla Società in fase decisoria non è stata

effettuata alcuna verifica in ordine al rispetto dei requisiti di sicurezza indicati nell'Allegato C al Regolamento SII.

45. L'Allegato 2 alla memoria di replica alle risultanze istruttorie, intitolato "Analisi di sicurezza cyber del sistema XBot", non supporta l'affermazione contenuta nella memoria di replica alle risultanze istruttorie secondo la quale il programma XBot non sarebbe idoneo – "*in sé, in virtù delle sue caratteristiche e delle sue funzioni*" – a determinare un *vulnus* alla sicurezza informatica del sistema (pag. 16 della memoria di replica alle risultanze istruttorie).
    Nella parte del parere dedicata alla "sicurezza del *software* del sistema XBot" (par. 1), il consulente di parte si è limitato, infatti, ad affermare che *nel momento in cui* è stata condotta l'analisi – e quindi non in via generale – non sono state evidenziate vulnerabilità del *software* ("*il rapporto di dettaglio non ha evidenziato vulnerabilità in atto*") e che dall'analisi sui componenti non sono stati rilevati "*errori degni di nota*".
46. Nel paragrafo 3 relativo alla "sicurezza del server SII", il consulente di Axpo si è limitato ad affermare che: a) "*tutte le interazioni del sistema XBot con il Sistema Informativo Integrato (SII) sono effettuate rispettando i protocolli di sicurezza*", senza specificare quali siano i protocolli di sicurezza presi a riferimento; b) che "*anche molteplici tentativi di interazione con il SII non costituiscono violazioni della sicurezza del sistema né sfruttamento di alcuna vulnerabilità che potrebbe danneggiare le funzionalità del sistema medesimo*", con ciò nulla aggiungendo alle risultanze istruttorie che, lungi dall'affermare la pericolosità intrinseca dei molteplici tentativi di interazione rilevati dal Gestore del SII il 17 luglio 2023, ha solo dato evidenza di come, da quei tentativi, AU abbia desunto l'operatività di un BOTNET (come poi ammesso dalla stessa Società); c) "*con riferimento alle tipologie di rischio evidenziate nell'Allegato C del Regolamento sul funzionamento del SII (…), nessuno dei potenziali rischi si è materialmente concretizzato a seguito del tentativo di accesso al SII mediante il tool XBot. In particolare, non vi è stata alcuna possibilità di violazione dell'integrità e della riservatezza dei dati come previsto in Sezione 2.2.: n. 4 Mantenimento dell'integrità dei dati; n. 5 – Assicurazione della riservatezza dei dati (…). Non vi è stata alcuna possibile concretizzazione delle principali categorie di rischio connesse al SII come menzionato in Sezione 2.3.*".
47. L'affermazione *sub* c) di cui al precedente alinea, in particolare, conferma, invece che smentire, la contestazione mossa alla Società. Anzitutto, la circostanza che "*nessuno dei potenziali rischi*" si sia "*materialmente concretizzato*" in un certo giorno è del tutto irrilevante, considerato che l'illecito contestato è un illecito di pericolo. È poi assai significativo che il consulente di parte, richiamando il par. 2.2. dell'Allegato C al Regolamento SII intitolato "Obiettivi di sicurezza del SII", abbia dovuto limitare l'affermazione secondo la quale "*non vi è stata alcuna possibilità di violazione dell'integrità e della riservatezza dei dati come previsto in sezione 2.2.*" ai soli obiettivi di sicurezza nn. 4 e 5 dell'elenco e non anche a quelli di cui ai nn. 1 (Identificazione delle entità), 2 (Autenticazione delle entità), 3 (Autorizzazione dei soggetti/applicazioni all'effettuazione delle operazioni), 6 (Non ripudio a livello di

richiesta e di risposta), 7 (Registrazione degli eventi/ispezione/Tracciabilità), 8 (amministrazione e Gestione della sicurezza).
Considerato che *tutti* gli obiettivi dell'elenco sono espressamente definiti come "*requisiti di sicurezza di carattere generale [che] dovranno essere contestualizzati, in fase di analisi e progettazione di dettaglio, per ciascun processo applicativo gestito tramite il SII e per i servizi e le componenti infrastrutturali, tra cui gli strumenti di comunicazione evoluta*", non si comprende come la Società possa sostenere che un sistema che non rispetta detti requisiti possa considerarsi conforme alla regolazione.

48. Infine, risulta generica e priva, dunque, di valore tecnico l'affermazione secondo la quale "*né vi è stata alcuna possibile concretizzazione delle principali categorie di rischio connesse al SII come menzionato in Sezione 2.3.*": i "rischi" elencati nella Tabella di cui al par. 2.3. dell'Allegato C al Regolamento SII sono infatti rischi di per sé associati alla gestione del SII – non si comprende quindi il senso di negarne la sussistenza – e ciò che è richiesto agli utenti del SII è che, rispetto a detti rischi, siano "*previste, attuate, verificate e aggiornate in continuo adeguate contromisure di natura fisica, logica e organizzativa*". Per tale ragione i sistemi possono interfacciarsi al SII solo per il tramite di PdC e di *Cloud Storage* e quindi sotto lo stretto controllo del Gestore del sistema, cosa che nel caso di specie non è avvenuta dal momento che il sistema XBot non risponde ai requisiti previsti per la comunicazione evoluta tra sistemi, a partire dalle modalità di autenticazione.
49. Priva di rilievo è altresì l'affermazione secondo la quale l'infrastruttura AXPO è stata valutata dal SII "*come rispondente agli standard richiesti in termini di monitoring, penetration test, access control e sicurezza durante la procedura di qualificazione del processo di scaricamento dati dal Cloud SII*". È evidente, infatti, che una cosa è il processo di scaricamento dati dal Cloud SII e altra cosa è il sistema XBot che accede al SII per il tramite del portale *web*, il quale non è stato oggetto di alcun controllo da parte del SII.
50. Quanto ai vantaggi che AXPO connette al sistema Xbot, premesso che i processi richiamati dall'esercente come non accessibili dalla porta di comunicazione sono in realtà marginali rispetto al complesso dei processi funzionali al normale svolgimento delle attività del venditore, l'eventuale aggiornamento dei processi accessibili dalla porta di comunicazione spetta al Gestore del SII, che detterà altresì tutte le necessarie misure di sicurezza.
51. Alla luce di quanto sopra, pure considerando tutte le repliche alla comunicazione delle risultanze istruttorie, devono confermarsi le conclusioni alle quali è pervenuto il Responsabile del procedimento all'esito della fase istruttoria.
52. In senso contrario non vale il richiamo alla buona fede. Come osservato dal Responsabile del procedimento, infatti, l'errore sulla liceità del fatto è rilevante e scriminante solo quando sussistano elementi positivi idonei a ingenerare nell'agente l'incolpevole opinione della liceità del suo agire, ciò che nel caso in esame non sussiste. E nel caso di specie non solo non sussiste alcun elemento positivo idoneo ad ingenerare un errore, ma la Regolazione è chiarissima nell'imporre agli Utenti del SII l'obbligo di rispettare specifiche misure di sicurezza a seconda del canale di

accesso prescelto, alle quali AXPO si è, almeno colpevolmente, sottratta utilizzando un BOTNET per l'accesso al SII tramite il portale *web*.

53. In definitiva, le circostanze dedotte dalla Società non sono idonee ad escluderne la responsabilità per la violazione degli articoli 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10, 6 comma 1 lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento, integrata dalla illegittima utilizzazione delle credenziali di accesso assegnate dal Gestore del SII ad un Utente finale (persona fisica dipendente di Axpo) tramite BOTNET non autorizzato.
54. La generica e non motivata richiesta di riservatezza del contenuto delle memorie difensive non può trovare accoglimento in considerazione di quanto previsto dall'articolo 7, comma 2, del Regolamento Sanzioni e Impegni.

QUANTIFICAZIONE DELLA SANZIONE:

55. L'articolo 11 della legge 689/81 dispone che la quantificazione della sanzione sia compiuta in applicazione dei seguenti criteri:
    a. gravità della violazione;
    b. opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze della violazione;
    c. personalità dell'agente;
    d. condizioni economiche dell'agente.
56. L'Autorità applica i criteri di cui al sopra citato articolo 11 alla luce di quanto previsto dagli articoli 29 e ss. del Regolamento Sanzioni.
57. Sotto il profilo della *gravità della violazione,* l'utilizzazione delle credenziali tramite BOTNET costituisce un illecito di pericolo e si pone in contrasto con le primarie regole di funzionamento del SII, poste a tutela dell'integrità dello stesso ovvero dei dati gestiti da un sistema informativo essenziale per il buon funzionamento dei mercati energetici, ossia affinché tutti i servizi regolati che confluiscono nel SII siano svolti in modo sicuro. La quantificazione della sanzione tiene conto del fatto che la violazione delle regole di sicurezza, a prescindere dalle dimensioni dell'operatore, costituisce comunque un *vulnus* per la sicurezza di un sistema informativo che rappresenta un'infrastruttura essenziale per il buon funzionamento dei mercati energetici e ciò sebbene – come nel precedente di cui alla deliberazione 479/2024/S/com – non risultino accertati concreti effetti pregiudizievoli sul mercato, sugli utenti, sui clienti finali e sull'azione amministrativa dell'Autorità, nonché indebiti vantaggi per Axpo. Inoltre, ai fini della valutazione in concreto della gravità della violazione, rilevano, oltre all'assenza di concreti effetti pregiudizievoli di cui si è appena detto, le seguenti circostanze: a) che non risulti accertata la cessione a terzi delle credenziali personali assegnate da AU ad un utente finale, persona fisica, per accedere al SII tramite portale *web* e che, dunque, la violazione consista nel solo utilizzo di dette credenziali per accedere al SII dal portale *web* attraverso il programma XBot; b) che – a differenza di quanto contestato nel procedimento chiuso con la deliberazione 479/2024/S/com richiamata da Axpo – le credenziali

illegittimamente utilizzate non siano quelle del responsabile della sicurezza. Sempre ai fini della valutazione della gravità rileva la circostanza che l'operatore sia di notevoli dimensioni e, dunque, possa accedere ad una rilevante mole di dati.

58. Non rileva invece ai fini della quantificazione della sanzione la circostanza che, a causa dell'attività di manutenzione del portale SII (e quindi per una causa peraltro estranea alla volontà dell'agente), il tentativo di accesso del 17 luglio 2023 sia "rimasto incompiuto"; a tal riguardo è sufficiente richiamare le ragioni già indicate ai punti 34 e 35.
59. Quanto alla durata, si dà atto che Acquirente Unico, nella relazione di cui al punto 3, ha rilevato che alla data del 22 febbraio 2024 non risultavano ulteriori eventi anomali (oltre a quello rilevato il 17 luglio 2023), in coerenza con quanto dichiarato da Axpo.
60. Costituendo l'illecito in argomento un illecito di pericolo, fermo quanto evidenziato al punto 57 quanto alla valutazione della concreta gravità della violazione, non ha uno specifico rilievo attenuante il mancato accertamento di concreti effetti pregiudizievoli sul mercato, sugli utenti, sui clienti finali e sull'azione amministrativa dell'Autorità, nonché di indebiti vantaggi per Axpo (considerato che gli illeciti sanzionati dall'Autorità sono tipicamente illeciti di condotta, l'art. 31, comma 1, lett. c) e d), del Regolamento Sanzioni si limita ad attribuire, infatti, uno specifico rilievo "aggravante" alla presenza di effetti pregiudizievoli e di indebiti vantaggi).
61. Sotto il profilo soggettivo, è sufficiente evidenziare che, ai sensi dell'art. 3 della legge 689/81, ai fini dell'integrazione dell'illecito amministrativo è sufficiente la colpa e che l'errore di diritto non ha efficacia scriminante, salvo quanto detto al precedente punto 52.
62. Con riferimento ai criteri dell'*opera svolta dall'agente per la eliminazione o attenuazione delle conseguenze della violazione* e della *personalità dell'agente*, non risultano circostanze rilevanti.
63. Sotto tale profilo non rileva, in particolare, la "spontanea rinuncia" all'utilizzo del programma XBot, costituendo la stessa mero atto dovuto (che peraltro non elimina né attenua le conseguenze della violazione ma ne evita il ripetersi).
64. Quanto alla assenza di reiterazione richiamata dalla Società nella memoria del 2 settembre 2024, si evidenzia anzitutto che, ai sensi dell'articolo 34 del Regolamento Sanzioni (cfr. anche art. 8 bis della legge 689/81), la "reiterazione" in senso tecnico rileva solo quando l'agente nei cinque anni successivi alla commissione di un illecito, accertata con provvedimento dell'Autorità, commetta un'altra violazione della stessa indole. Non rileva, invece, l'assenza della "reiterazione" in senso tecnico, così come non rileva, ai sensi del medesimo Regolamento Sanzioni, l'assenza di precedenti, non potendo assumere valore attenuante la condotta che si esaurisce, né più né meno, nell'avere – presumibilmente e fino al momento dell'adozione di un provvedimento sanzionatorio – rispettato gli obblighi posti in capo a tutti gli operatori che svolgano una certa attività.
65. Quanto alla dedotta collaborazione nell'attività istruttoria richiamata nella memoria del 2 settembre 2024, non si ravvisa un livello di cooperazione efficace ai sensi dell'art. 33 comma 2, lettera b) del Regolamento Sanzioni, non avendo fornito la

Società nel corso del procedimento elementi a sé sfavorevoli diversi da quelli già rilevati dall'Autorità.

66. Non rileva, infine, l'intenzione della Società di adottare un disciplinare interno per rafforzare il grado di consapevolezza dei propri dipendenti circa le norme che regolano il SII (circostanza richiamata nella memoria del 2 settembre 2024 e a supporto della quale la Società ha svolto repliche alle risultanze istruttorie). Deve infatti confermarsi quanto già affermato dal Responsabile del procedimento, ossia che, in disparte la mancata dimostrazione dell'attuazione di tale misura, come rilevato nella deliberazione 268/2024/S/com di inammissibilità della proposta di impegni, rientra, infatti, tra gli obblighi di ciascun Utente del SII quello di adottare ogni misura organizzativa necessaria a garantire il rispetto delle disposizioni del Regolamento del SII. Né può seriamente pretendersi che una circostanza considerata irrilevante in una sede (valutazione degli impegni), poiché consistente nel mero adempimento di un obbligo posto dalla Regolazione, possa poi rilevare in un'altra (quantificazione della sanzione) per il solo fatto che detta valutazione condurrebbe a risultati diversi, ma sempre favorevoli all'esercente (diverso sarebbe stato il caso in cui l'inammissibilità degli impegni fosse stata giustificata, per esempio, dalla mancata cessazione della violazione, ritenendosi invece nella sostanza meritevole di apprezzamento la condotta oggetto della stessa proposta di impegni).
67. Per quanto attiene alle *condizioni economiche dell'agente*, nella lettera di trasmissione della memoria del 6 dicembre 2024, la Società ha comunicato la propria situazione contabile al 30 settembre 2024. Preso atto dei ricavi realizzati dalla Società nel 2024 (confermati dal bilancio 2023 acquisito d'Ufficio in fase decisoria, laddove la Società si era impegnata ad inviare il bilancio dopo l'approvazione da parte dell'assemblea dei soci), si evidenzia che ai sensi dell'articolo 32 del Regolamento Sanzioni (in coerenza con l'art. 45 del decreto legislativo 93/11), le condizioni economiche dell'agente si ricavano dal fatturato realizzato nell'ultimo esercizio *chiuso* prima dell'avvio del procedimento sanzionatorio e si desumono quindi, nel caso di specie, dal bilancio relativo all'anno 2023, dal quale risultano ricavi pari a euro 6.918.834.560.
68. Per tutto quanto sopra la sanzione può essere determinata in euro 1.225.000,00 (unmilioneduecentoventicinquemila/00)

DELIBERA

1. di accertare la violazione, da parte di Axpo Italia S.p.A., nei termini di cui in motivazione, degli articoli dell'articolo 6, comma 1, lettera d) dell'Allegato A alla deliberazione ARG/com 201/10, e degli articoli 6, comma 1, lettera c) e 15, comma 3, del Regolamento del SII, nonché delle sezioni 2.2 e 2.4 dell'allegato C al medesimo Regolamento;
2. di irrogare, nei confronti di Axpo Italia S.p.A., ai sensi dell'articolo 2, comma 20, lettera c), della legge 481/95, una sanzione amministrativa pecuniaria di euro

1.225.000,00 (unmilioneduecentoventicinquemila/00) per la violazione degli articoli di cui al precedente punto 1;

3. di ordinare a Axpo Italia S.p.A. di pagare la sanzione irrogata entro il termine di 30 giorni dalla data di comunicazione del presente provvedimento, tramite versamento da effettuarsi mediante l'utilizzo del servizio PagoPA, disponibile nella sezione "*Comunicati per operatori*" del sito istituzionale dell'Autorità (al link: https://www.arera.it/comunicati-operatore/dettaglio/pagamento-sanzioni-tramite-pagopa-25), selezionando nel "Dettaglio pagamento" il "Fondo Sanzioni Arera" e indicando, nel campo causale: "Fondo Sanzioni Arera deliberazione 106/2025/S/com";
4. di avvisare che, decorso il termine di cui al precedente punto 3, per il periodo di ritardo inferiore ad un semestre, devono essere corrisposti gli interessi di mora nella misura del tasso legale a decorrere dal giorno successivo alla scadenza del termine del pagamento e sino alla data del pagamento; in caso di ulteriore ritardo nell'adempimento, saranno applicate le maggiorazioni di cui all'articolo 27, comma 6, della legge 689/81;
5. di comunicare il presente provvedimento a Axpo Italia S.p.A. (P.IVA 01141160992), mediante pec all'indirizzo segreteria@pec.axpoitalia.biz, nonché agli avvocati Maurizio Pappalardo e Pasquale Leone, rispettivamente agli indirizzi pec mkpappalardo@pec.it e pasqualeleone@ordineavvocatiroma.org, e di pubblicarlo sul sito internet dell'Autorità www.arera.it.

Avverso il presente provvedimento può essere proposto ricorso dinanzi al competente Tribunale Amministrativo Regionale della Lombardia, sede di Milano, entro il termine di 60 giorni dalla data di notifica dello stesso oppure ricorso straordinario al Capo dello Stato, entro il termine di 120 giorni.

25 marzo 2025

IL PRESIDENTE
Stefano Besseghini