G L 0 D U W H G u J H Q Q D L R

Sommario Rassegna Stampa

Il Sole 24 ORE

Quotidiano Data 30-01-2024
Pagina 1
Foglio 1 / 2

INTELLIGENZA ARTIFICIALE

Garante privacy contro OpenAI: viola le regole sui dati personali

Alessandro Galimberti —a pag. 18

Faro su OpenAI. Il Garante privacy notifica ai proprietari di ChatGPT un atto di contestazione

Privacy, il Garante a OpenAI: violate le regole sui dati personali

Intelligenza artificiale

Per l'Autorità commessi uno o più illeciti rispetto a quanto stabilito dal Regolamento Ue

I proprietari di Chatgpt ora hanno 30 giorni di tempo per difendersi dalle accuse

Alessandro Galimberti
MILANO

Il secondo capitolo del braccio di ferro tra il Garante della privacy e OpenAI si chiude con una lettera formale di contestazioni e 30 giorni di tempo, per i proprietari di Chatgpt, per difendersi dall'accusa di violazione seriale delle regole italiane (ed europee) sulla privacy.

La traumatica limitazione del servizio di "intelligenza artificiale" adottata nella primavera scorsa dall'authority di piazza Venezia - che aveva trascinato con sè anche il Comitato europeo per la protezione dei dati (Edpd) e portato il caso a Bruxelles - non aveva infatti chiuso la partita con Open Ai, nonostante l'*agreement* del 28 aprile successivo che sembrava aver diradato le incomprensioni.

In realtà il Garante, quando prese atto dell'allineamento di Chaptgpt alle condizioni di servizio minime e tornò perciò a sbloccarlo, si era riservato di perseguire quanto avvenuto nei mesi (anni?) precedenti a danno dei diritti di inconsapevoli cittadini/utenti. E l'ora del *redde rationem* è scattata ieri, con la notifica formale delle contestazioni.

Per comprendere la posta in gioco - che in teoria potrebbe ancora portare a sanzioni nell'ordine del 4% del fatturato globale dell'azienda americana - è opportuno tornare alla scorsa primavera e alle contestazioni di allora. A partire dalla richiesta di predisposizione sul sito, come del resto prevede il *Global data protection regulation* (Gdpr, in vigore in tutta l'Unione) di un'informativa trasparente con le modalità e la logica alla base del trattamento dei dati necessari al funzionamento di ChatGPT «nonché i diritti attribuiti agli utenti e agli interessati non utenti». Informativa che deve essere presentata prima del completamento della registrazione, insieme alla dichiarazione di maggiore età dell'utente. La seconda azione richiesta a ChatGpt era di cambiare la base giuridica: non più il contratto di servizio ma il consenso o il legittimo interesse quale presupposto per utilizzare i (preziosissimi) dati degli utenti. Ancora, la piattaforma era chiamata a consentire agli utenti (e anche a terzi non utenti) di ottenere facilmente la rettifica dei dati personali trattati e, prima ancora, l'opposizione *tout court* al loro utilizzo. Infine, a Chat Gpt venne imposto in quella occasione di presentare un sistema di *age verification* in grado di escludere l'accesso agli utenti sotto i 13 anni e ai minorenni senza il consenso dei genitori.

Misure, quelle richieste, alle quali OpenAi si era in larga misura adeguata in meno di 60 giorni - dall'informativa al diritto di opposizione fino alla cancellazione dei dati scorretti (con qualche riserva sulla fattibilità tecnica) e alla dichiarazione di maggiore età o di consenso dei genitori, consentendo la riapertura piena del servizio, ma con l'ulteriore invito a rafforzare il controllo sull'accesso di minorenni.

Sullo sfondo della partita italiana si staglia la non meno impattante iniziativa varata sempre la scorsa primavera dal Comitato europeo per la protezione dei dati (Edpd) per creare «politiche generali che siano trasparenti» in materia di Ai. Il Comitato prese atto che rilievi mossi dall'authority italiana al funzionamento di ChatGpt in materia di privacy erano seri, profondi, e soprattutto comuni, e aveva scelto la strada del rafforzamento della cooperazione tra le Authorities dello spazio unionale mettendo in campo una task force. Ora i lavori di quel gruppo d'azione diventeranno la cartina di tornasole anche per la soluzione della controversia-madre, che andrà in scena a Roma.

LA PROCEDURA

4%

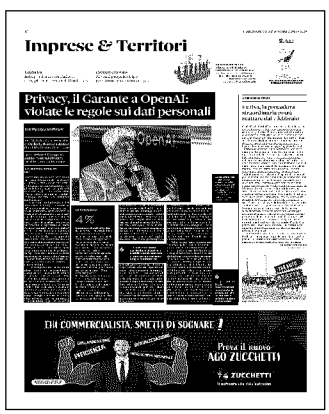
La sanzione sul fatturato
Il Garante della privacy italiano ha aperto una procedura di contestazione contro OpenAi, proprietaria di Chatgpt, per la violazione seriale di diverse norme del Gdpr, il regolamento europeo di protezione dei dati personali. La società americana, che si era già vista sospendere il servizio nella primavera scorsa per questi motivi, rischia una sanzione che nei casi gravi può essere calcolata anche sul giro d'affari e può raggiungere il 4% del fatturato globale.
Il 28 aprile del 2023, due mesi dopo il blocco di Roma - e l'avvio nel frattempo di una task force dei garanti europei sul tema - OpenAi aveva raggiunto un accordo di allineamento con il Garante, lasciando però impregiudicato iquanto avvenuto in passato.

Tra le azioni chieste quella di cambiare base giuridica: no al contratto di servizio ma consenso o legittimo interesse

LE QUESTIONI
Tra le contestazioni la richiesta di predisposizione sul sito di un'informativa trasparente

La posta in gioco. In teoria tutto questo potrebbe portare a sanzioni nell'ordine del 4% del fatturato globale dell'azienda americana (nella foto il ceo Sam Altman)


Il Sole 24 ORE
Bce e tassi, taglio ad aprile più vicino
Confindustria: in miglioramento le aspettative sulla crescita


Imprese & Territori
Privacy, il Garante a OpenAI: violate le regole sui dati personali
4%
EH COMMERCIALISTA, SMETTI DI SOGNARE !
Prova il nuovo AGO ZUCCHETTI

Il Sole 24 ORE

Quotidiano Data 30-01-2024
Pagina 38
Foglio 1 / 3

Fondazione Bruno Visentini

SULLA CYBERSICUREZZA MEGLIO L'INTELLIGENCE CHE LE SANZIONI PIÙ SEVERE

di **Andrea R. Castaldo**

Il disegno di legge cybersecurity, approvato la scorsa settimana dal Consiglio dei ministri, conferma l'attenzione crescente e la consapevolezza dei rischi che si nascondono dietro la criminalità informatica. Una macrocategoria, convenzionalmente racchiusa sotto l'insegna aggregante dei computer crimes, in realtà aperta a ventaglio in svariate e diverse fattispecie delittuose. Caratteristica che rende più difficile aggredirla, in virtù delle strategie di repressione da differenziare.

Ma andiamo per ordine. Negli ultimi due anni molteplici sono state le novità in tema di sicurezza cibernetica, compresa tra i progetti finanziati dal Pnrr. Tra le disposizioni urgenti in materia di processo penale, figura l'articolo 2-bis del Dl 105/2023 (convertito con modificazioni dalla legge 137/2023), che si prefigge l'obiettivo di innalzare i livelli di cybersicurezza e di implementare gli strumenti di repressione dei crimini informatici, estendendo le misure di contrasto a oggi ristrette alla criminalità organizzata e al terrorismo.

Particolarmente interessanti le norme volte a espandere l'area delle operazioni *under cover* (con annesse prerogative) per il contrasto del cybercrime.

Il percorso tracciato viene ripreso e consolidato con il Ddl di questi giorni, le cui linee portanti si riassumono – in buona sostanza – nella consueta politica dello *stick and carrot*. Miscela divenuta costante nella risposta a fenomenologie criminali nuove o preesistenti mutate geneticamente. E allora, sul versante repressivo, l'inevitabile aumento della pena trova conferma nei reati connessi alla violazione dei dati informatici. La sanzione della reclusione, prevista dall'articolo 615-ter del Codice penale per alcuni reati informatici, si estende infatti «da due a dieci anni» (anziché «da uno a cinque anni»). Nei casi in cui i reati commessi riguardino «sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico», la reclusione varia «da tre a dieci anni e da quattro a 12 anni».

In materia di intercettazione, si inasprisce la pena detentiva dell'articolo 617-quater del Codice penale: «da quattro a dieci anni» e non più da «tre a otto anni».

L'altrettanto collaudato meccanismo del "tendere la mano" si ritrova nella nuova figura dell'hacker pentito. Le pene «sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi».

È difficile prevedere efficacia e portata applicativa di tali misure, stante la peculiarità criminologica del tipo d'autore e della natura del reato. La cybercriminalità ha caratteristiche specifiche. Nessun confine geografico, nessun testimone, nessuna temporalità, con spiccate se non esclusive origini e finalità economiche. L'hacker si muove nell'anonimato, in una rete di complicità diffusa e con condotte seriali e su larga scala, il che assicura una buona dose di impunità. E per converso lo Stato deve investire ingenti risorse tecnologiche in termini di uomini e mezzi per l'accertamento del reato e l'individuazione dei responsabili. Pentirsi e collaborare implica una convenienza (la famosa «controspinta alla spinta psicologica») altrettanto forte e difficile da immaginare.

Per le medesime ragioni la deterrenza sanzionatoria rischia di non colpire nel segno. Semmai è la spia della riconosciuta insidiosità di tali reati e della correlata aggressione a beni giuridici di preminente interesse nella scala costituzionale dei valori.

E qui è utile distinguere nuovamente. Accanto a forme tradizionali e meno pericolose (truffe informatiche), semmai particolarmente odiose

Nihil *novi sub sole*. Il

Fondazione Bruno Visentini

SULLA CYBERSICUREZZA MEGLIO L'INTELLIGENCE CHE LE SANZIONI PIÙ SEVERE

di **Andrea R. Castaldo**

Nihil novi sub sole. Il disegno di legge cybersecurity, approvato la scorsa settimana dal Consiglio dei ministri, conferma l'attenzione crescente e la consapevolezza dei rischi che si nascondono dietro la criminalità informatica. Una macrocategoria, convenzionalmente racchiusa sotto l'insegna aggregante dei computer crimes, in realtà aperta a ventaglio in svariate e diverse fattispecie delittuose. Caratteristica che rende più difficile aggredirla, in virtù delle strategie di repressione da differenziare.

Ma andiamo per ordine. Negli ultimi due anni molteplici sono state le novità in tema di sicurezza cibernetica, compresa tra i progetti finanziati dal Pnrr. Tra le disposizioni urgenti in materia di processo penale, figura l'articolo 2-bis del Dl 105/2023 (convertito con modificazioni dalla legge 137/2023), che si prefigge l'obiettivo di innalzare i livelli di cybersicurezza e di implementare gli strumenti di repressione dei crimini informatici, estendendo le misure di contrasto a oggi ristrette alla criminalità organizzata e al terrorismo.

Particolarmente interessanti le norme volte a espandere l'area delle operazioni *under cover* (con annesse prerogative) per il contrasto del cybercrime.

Il percorso tracciato viene ripreso e consolidato con il Ddl di questi giorni, le cui linee portanti si riassumono – in buona sostanza – nella consueta politica dello *stick and carrot.* Miscela divenuta costante nella risposta a fenomenologie criminali nuove o preesistenti mutate geneticamente. E allora, sul versante repressivo, l'inevitabile aumento della pena trova conferma nei reati connessi alla violazione dei dati informatici. La sanzione della reclusione, prevista dall'articolo 615-ter del Codice penale per alcuni reati informatici, si estende infatti «da due a dieci anni» (anziché «da uno a cinque anni»). Nei casi in cui i reati commessi riguardino «sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico», la reclusione varia «da tre a dieci anni e da quattro a 12 anni».

In materia di intercettazione, si inasprisce la pena detentiva dell'articolo 617-quater del Codice penale: «da quattro a dieci anni» e non più da «tre a otto anni».

L'altrettanto collaudato meccanismo del "tendere la mano" si ritrova nella nuova figura dell'hacker pentito. Le pene «sono diminuite dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi dei delitti o degli strumenti utilizzati per la commissione degli stessi».

È difficile prevedere efficacia e portata applicativa di tali misure, stante la peculiarità criminologica del tipo d'autore e della natura del reato. La cybercriminalità ha caratteristiche specifiche. Nessun confine geografico, nessun testimone, nessuna temporalità, con spiccate se non esclusive origini e finalità economiche. L'hacker si muove nell'anonimato, in una rete di complicità diffusa e con condotte seriali e su larga scala, il che assicura una buona dose di impunità. E per converso lo Stato deve investire ingenti risorse tecnologiche in termini di uomini e mezzi per l'accertamento del reato e l'individuazione dei responsabili. Pentirsi e collaborare implica una convenienza (la famosa «controspinta alla spinta psicologica») altrettanto forte e difficile da immaginare.

Per le medesime ragioni la deterrenza sanzionatoria rischia di non colpire nel segno. Semmai è la spia della riconosciuta insidiosità di tali reati e della correlata aggressione a beni giuridici di preminente interesse nella scala costituzionale dei valori.

E qui è utile distinguere nuovamente. Accanto a forme tradizionali e meno pericolose (truffe informatiche), semmai particolarmente odiose perché dirette verso persone fragili, il baricentro della preoccupazione sposta il proprio asse verso condotte in grado di carpire segreti inerenti alla sicurezza nazionale o danneggiare reti informatiche strategiche. Un genere di criminalità che vanta un'organizzazione ramificata e collaudata, sulla base di precise direttive e persino indirizzi governativi, come inchieste internazionali hanno dimostrato.

Se in astratto l'opzione di

severità punitiva è giustificata dai valori in gioco che si possono spingere fino alla tenuta dell'ordine democratico, è altrettanto chiaro in concreto come l'attività di intelligence e di prevenzione rivesta un ruolo fondamentale.

Prevenzione che si declina in una duplice prospettiva: contenitiva, cioè dotarsi degli strumenti tecnici e dei programmi di sicurezza per impedire l'attacco, proattiva, nel senso di un costante monitoraggio e alert di obiettivi sensibili, finalizzati al riconoscimento precoce dell'hacker. L'intelligenza artificiale si rivela allora un alleato prezioso e lo sarà ancora di più in un futuro ravvicinato, capace come è di elaborare abilità predittive e strategie di contrasto tarate sull'individualità.

Ordinario di Diritto Penale
Università degli Studi di Salerno
Osservatorio Fondazione Bruno Visentini

SICUREZZA NAZIONALE
Severità punitiva giustificata dai valori in gioco ma la prevenzione funziona di più

PREVENZIONE
L'intelligenza artificiale può sviluppare capacità predittive e strategie di contrasto tarate sull'individualità


Crediti d'imposta, il quadro RU diventa più leggero da Redditi 2024

COLF E BADANTI

CORRIERE DELLA SERA

Quotidiano Data 30-01-2024
Pagina 35
Foglio 1

Il gruppo ucraino

di **Federico Fubini**

«Acciaio, così Metinvest rilancerà Piombino Taranto? Valuteremo»

Il ceo Ryzhenkov: un errore importare dalla Russia

Metinvest si sta impegnando con forza nell'acciaieria di Piombino. Con quali piani?

«Siamo presenti in Italia da 15 anni. E i piani per una nuova produzione di acciaio verde in Italia sono nati prima che la Russia scatenasse l'invasione totale due anni fa — risponde Yuriy Ryzhenkov, amministratore delegato del colosso ucraino dell'acciaio Metinvest —. All'inizio volevamo costruire un impianto che utilizzasse le bramme di Azovstal, che è di nostra proprietà, per produrre laminati a caldo in Italia. Ma dopo la tragedia di Mariupol, abbiamo optato per un impianto di produzione a Piombino. Il progetto è quello dell'acciaio verde, progettato per utilizzare il preridotto dai nostri impianti di minerale di ferro in Ucraina. Sarà un esempio di un nuovo impianto che potrà fare da pilota sia in Europa che in Ucraina. Investire adesso in Ucraina è difficile. Quindi abbiamo deciso di iniziare dall'Italia e dar prova del modello. Poi potremo estenderlo ad altri siti».

Le norme ambientali europee richiedono investimenti massicci. Pensate di poter beneficiare di aiuti pubblici?

«Investiremo a Piombino una notevole quantità di capitale, sia di Metinvest che del nostro partner Danieli. Ma cercheremo il sostegno di operatori finanziari sia istituzionali che commerciali. Esistono diversi fondi ambientali italiani e comunitari da utilizzare, se il nostro progetto apporta benefici ambientali. Sarà un mix di capitale proprio, debito e prestiti o sussidi di fondi pubblici».

Taranto è la seconda acciaieria d'Europa dopo Azovstal. Investirebbe su Taranto, a fianco del governo italiano, per sostituire la capacità persa a Mariupol?

«Taranto era anche più grande di Azovstal, penso fosse l'impianto più grande d'Europa. Oggi è molto sotto alla sua capacità, ma il potenziale ci sarebbe. E il governo italiano ha detto che sta cercando investitori privati».

Dunque state guardando a questa opzione?

«Il nostro progetto a Piombino non nasce solo dalla necessità di sostituire Mariupol, ma dal mercato. L'Italia oggi importa più di sei milioni di tonnellate di laminati a caldo all'anno. Quindi in Italia c'è un grande bisogno di questo prodotto, il che significa che anche a Taranto c'è spazio per aumentare la produzione. Il mercato c'è. Al momento siamo fornitori di materie prime per Taranto e acquirenti di bramme da lì per i nostri impianti di laminazione italiani. E il nostro obiettivo primario in questo momento è Piombino. Poi col passare del tempo, se vediamo un'opportunità su Taranto, perché no? Possiamo guardarci. Ma per ora siamo concentrati solo su Piombino».

L'Italia non è semplice. Vorreste che il governo si impegnasse a facilitare l'investimento, sia a Piombino, sia prima di valutare Taranto?

«Siamo in Italia da 15 anni, sappiamo come funziona. Su Piombino c'è un ottimo impegno da parte del governo, della regione e del sindaco. Tutti tengono al progetto. Nel memorandum firmato, ciascuna delle parti si è impegnata a fornire un certo sostegno. È un buon inizio, anche se comprendiamo le complessità del sistema. Ma se lavoriamo tutti insieme, possiamo creare un ambiente favorevole. Abbiamo scelto Piombino perché abbiamo riscontrato un altissimo impegno e interesse da parte di tutti».

Su Taranto, lei dice che vuole vedere se c'è un'«opportunità». Ossia, se dalle autorità c'è un impegno simile a quello di Piombino?

«Assolutamente. Taranto è un caso molto difficile. Lì esiste un investitore e il governo sta lavorando per risolvere quel caso. Poi ci sono i problemi con le autorità locali, le questioni ambientali, quelle occupazionali... Ci sono molti problemi e non credo che un singolo attore possa risolverli tutti. Ora il governo ci sta lavorando e bisognerà vedere che tipo di accordo verrà messo in atto. Se il governo vorrà coinvolgere altri soggetti, dovremo valutare attentamente. E se possiamo aiutare, ci proveremo».

L'Ue non ha ancora sanzioni totali sull'acciaio russo. Che ne pensa?

«La cosa è ancora più tragica perché all'inizio c'era una deroga alle sanzioni sull'importazione di bramme russe, che scadeva più o meno ora. Poi, di recente, è stata prorogata per sei anni. Dicono che non riescono a sostituire il materiale russo. Secondo me, non è vero. Noi produciamo un milione di tonnellate di prodotti piatti all'anno in Europa e circa 200 mila nel Regno Unito. E siamo riusciti a sostituire la produzione di Azovstal senza comprare nulla dai russi. Permettendo le importazioni russe, in Italia ci stiamo sparando sui piedi, perché il progetto di Taranto diventa ancora più difficile dato che deve competere con materiale russo in genere molto meno caro».

Chi importa bramme russe?

«I principali compratori sono in Italia e Belgio».

L'ex Ilva
Nell'ex Ilva il potenziale ci sarebbe. Anche perché l'Italia importa 6 milioni di tonnellate l'anno

Yuri Ryzhenkov