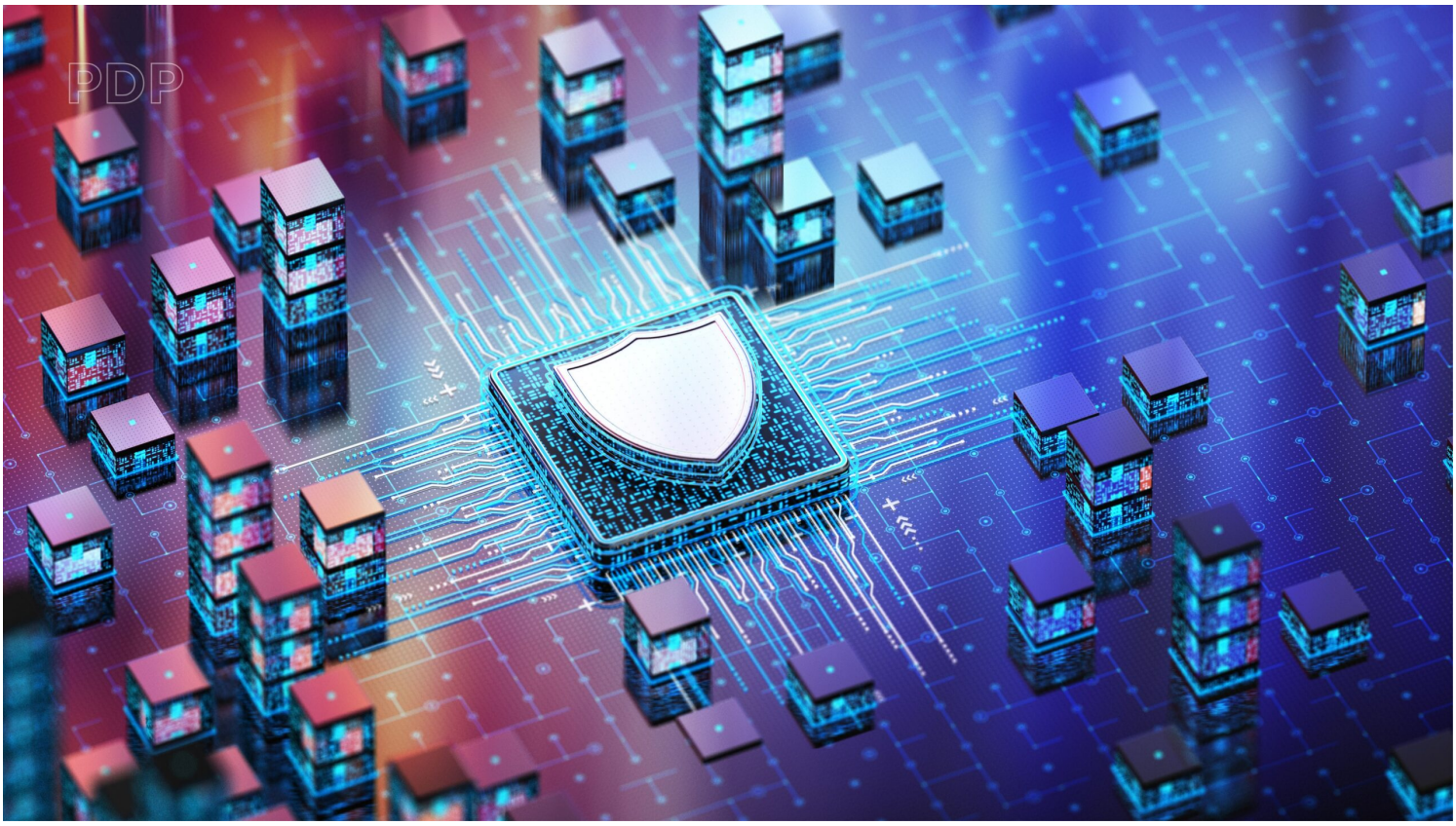
CHIEDETE E VI SARÀ 'DATO'. DISILLUSE OSSERVAZIONI PENALISTICHE A PROPOSITO DI (IN)SICUREZZA INFORMATICA

Stefano Fiore



Non abbiamo elementi per stabilire se l'indagine della Procura di Perugia, mediaticamente presentata, in maniera probabilmente impropria, come avente ad oggetto una presunta attività di dossieraggio, ha davvero scoperchiato, per usare le parole del Procuratore Cantone, un 'verminaio'. Ma anche indipendentemente da quelli che saranno gli esiti del procedimento penale, gli scenari che si schiudono alla nostra vista sono fonte di inquietudine e non pochi, né di poco momento sono gli interrogativi che li accompagnano.

Anche se i contorni della vicenda restano allo stato abbastanza fumosi, dalle notizie disponibili è infatti emersa quella che si presume essere stata una vasta e sistematica violazione di numerose banche dati in

uso alla Procura Nazionale Antimafia, mediante accessi abusivi ai sistemi informatici al fine di ottenere notizie riservate o comunque personali relative a politici, imprenditori, sportivi.

Pur non essendo ancora chiaro in vista di quale o quali finalità sia avvenuta la raccolta abusiva dei dati, è comunque ovvio che la vulnerabilità dei sistemi organizzati di archiviazione delle informazioni in uso all'autorità giudiziaria e agli organi investigativi per ragioni connesse all'esercizio delle loro funzioni, è una circostanza che suscita preoccupazione e giustificato allarme.

Il modo in cui l'enorme mole di dati che riguarda tutti noi viene raccolta, gestita e utilizzata rappresenta infatti da tempo una delle variabili dalle quali nella società contemporanea dipende la sorte 'reale' dei diritti individuali e dunque la futura qualità dei sistemi democratici.

Nell'ambito della più vasta rivoluzione digitale in atto, nel 'potere dei dati' è riconoscibile una spiccata e ormai sperimentata attitudine a ridefinire il rapporto tra tecnica e democrazia. La conferma possiamo trarla guardando a quel che già avviene nei sistemi non democratici, dove è non solo inequivoco, ma si potrebbe dire 'palese' quale sia l'enorme ruolo che le basi di dati svolgono nella gestione autoritaria delle funzioni di controllo sociale.

Inoltre, la circostanza che, sempre sulla base di ciò che è stato reso noto, alcune delle notizie riservate illecitamente raccolte sarebbero state veicolate ad organi di informazione, andando a costituire materiale per inchieste giornalistiche, determina il coinvolgimento in questa già complessa vicenda dei delicati equilibri che, sempre negli ordinamenti democratici, derivano dalla necessità di garantire e tutelare la libertà di stampa.

Per l'insieme delle accennate ragioni, appare quindi comprensibile che l'indagine abbia suscitato un particolare clamore, alimentato anche dalla non usuale decisione del Procuratore della Repubblica di Perugia e del Procuratore Nazionale Antimafia di farsi audire dalla Commissione parlamentare antimafia e dal Copasir, per riferire su quanto sinora accertato. Proprio questo clamore, che invero si va lentamente spegnendo, ha favorito tuttavia anche il diffondersi di imprecisioni ed equivoci, offrendo facile occasione, dato il contesto e i protagonisti, anche per strumentalizzazioni immediatamente trasferite sul terreno del confronto politico.

Sono dunque numerosi, intrecciati e complessi i piani sui quali sarebbe possibile collocarsi per analizzare ed

eventualmente commentare quanto sta avvenendo. Su molti di questi piani le questioni che si rinvengono sono ovviamente anche di diretto interesse per il penalista e non si limitano a quelle immediatamente collegate alle investigazioni in corso, che definiscono, allo stato, la cornice cognitiva (e comunicativa) entro la quale la vicenda risulta iscritta.

Il non formale richiamo alla necessità di un rigoroso rispetto della presunzione di non colpevolezza, esclude tuttavia che in questa sede, come auspicabilmente anche in altre, si possa svolgere qualsiasi considerazione di merito che prescinda dalla doverosa attesa degli esiti definitivi degli accertamenti processuali.

Le brevissime considerazioni che intendo svolgere si limitano pertanto ad assumere i fatti sui quali si sta indagando solo come spunto - invero di particolare rilievo come subito si dirà - per riflettere, ancora una volta, sul ruolo del diritto penale e soprattutto sul modo in cui il suo uso, attuale o futuro, viene percepito e come tale percezione venga trasferita in particolare nella comunicazione e anche nella concreta azione politica.

Non è dato sapere se la dimensione e la gravità dei fatti oggetto indagine saranno ridimensionate ed eventualmente in che misura oppure se, al contrario, il quadro finale sarà di gravità estrema, con implicazioni ad oggi ancora non note, ma in entrambi i casi dal punto di vista penalistico non cambierebbe moltissimo. Al netto della possibilità che emergano ulteriori profili di rilevanza penale (ad esempio corruzione o altro) la incommensurabile distanza tra la enorme complessità del fenomeno e le modeste possibilità di intervento degli strumenti penali, costretti a ritagliare, con fatica, minuscole 'figurine' da un gigantesco affresco, apparirà in tutta la sua impietosa evidenza.

L'indagine della Procura perugina ruota, infatti, attorno a condotte astrattamente riconducibili al delitto di accesso abusivo a sistemi informatici (art. 615 *ter* c.p.), fattispecie che necessita senz'altro di un'accurata revisione e che nella versione attuale copre uno spettro di fatti molto vario, prevedendo (anche per questo motivo) sanzioni di misura non particolarmente elevata. Per il resto si lavora con i vecchi arnesi del falso e, addirittura, con la 'moribonda' ipotesi di cui all'art. 323 c.p.

Questo banale rilievo dovrebbe suggerirci qualcosa che, nonostante sia manifesto, vale forse la pena, ancora una volta, esplicitare: la circostanza che determinati fatti abbiano o possano assumere (eventuale) rilevanza penale non consente 'di per sé' di identificare e soprattutto di esaurire il loro significato nella dimensione penalistica, affidando quindi agli strumenti del diritto criminale il compito di trovare le soluzioni.

Si è sopra accennato alla eccezionale complessità dell'orizzonte entro il quale si iscrive la fondamentale questione della sicurezza dei 'dati', in considerazione del ruolo che essi svolgono nel (ri)definire modelli sociali, assetti economici e addirittura geopolitici.

Rispetto alla portata di tali questioni, il massimo che si può chiedere al sistema penale è di provare a migliorare le *performances* descrittive di alcune fattispecie incriminatrici e adeguare alcuni dei suoi strumenti processuali.

Come spesso accade, una singola vicenda, in ragione delle sue peculiarità o del momento storico nel quale si colloca, dando visibilità ad un problema (evidentemente già esistente) mette in moto, non sempre in maniera ordinata, meccanismi legislativi di riforma/adeguamento delle discipline di settore.

Questo riflesso condizionato è immediatamente scattato anche a seguito dall'*input* fornito dalla confusa *spy story* dalle quale queste osservazioni traggono spunto.

Posti di fronte alle manifeste carenze delle misure di *cybersecurity* in settori cruciali, i decisori politici avevano a disposizione una ennesima e ottima occasione per testare la loro capacità e ancor prima la loro volontà di resistere, in tempi di imperante panpenalismo, alla tentazione di affidarsi alla facile reazione istintiva di una risposta a forte o prevalente connotazione penale.

Orbene, il test non sembra essere stato superato neppure questa volta.

In sostanziale coincidenza temporale con la esplosione mediatica di una indagine la cui esistenza era in realtà nota da diversi mesi, il Governo ha presentato alla Camera un DDL (Atto Camera N. 1717 - Presentato il 16 febbraio 2024[1]), contenente «Disposizioni *in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*».

Il provvedimento contiene innanzitutto (e ci mancherebbe altro!) una serie di misure destinate al «rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici».

Tali misure sono destinate, nelle intenzioni del legislatore, a «sviluppare capacità nazionali di prevenzione, monitoraggio, rilevamento, analisi e risposta, per prevenire e gestire gli incidenti di sicurezza informatica e gli attacchi informatici».

È impossibile dire, tra l'altro senza analizzarle, quale potrà essere, se e quando le relative disposizioni verranno approvate, il contributo che le misure proposte sono in grado di offrire ad un effettivo miglioramento della *cybersecurity* nazionale. L'impressione però è che il legislatore abbia ceduto anche in questo caso al ricorrente vizio di privilegiare un approccio di tipo 'procedurale', ma in attesa di vedere il modello in funzione (se mai ciò accadrà), il giudizio non può che essere sospeso.

Quel che invece è certo è che il Capo II del citato DDL prevede un corposo intervento di riforma dei reati informatici, strutturato secondo il consueto e consunto schema dell'inasprimento sanzionatorio, realizzato direttamente operando sulla misura delle pene o attraverso meccanismi di blindatura delle circostanze, il cui novero è stato peraltro ulteriormente incrementato. Non manca poi la proposta di introdurre, assecondando una sorta di ossessione casistica a tinte fortemente simboliche, nuove ipotesi di reato che specializzano figure già esistenti e tra le quali si segnala una inedita figura di 'estorsione informatica', la cui pena massima, per le ipotesi aggravate, arriva fino a ventidue anni di reclusione.

Altrettanto immancabile, secondo il collaudato schema adottato in gran parte della recente legislazione penale è poi anche la parallela attivazione di alcuni tratti processuali a doppio binario sui quali instradare in futuro anche i reati informatici.

Senza dimenticare, infine, che la chiusura del DDL resta affidata, come sempre, ad una clausola di invarianza finanziaria, pur essendo di tutta evidenza che mai come in questo caso sarebbe necessario investire cospicue risorse per i necessari aggiornamenti tecnologici, il reclutamento di adeguate competenze e la formazione del personale.

La necessità che il nostro ordinamento, anche penale, sia più pronto e, per così dire, anche più preciso, nell'adeguarsi ai nuovi paradigmi di realtà indotti e anzi imposti dalla rivoluzione digitale è cosa fuor di dubbio. Quando il cammino parlamentare di questo disegno di legge sarà concluso (se sarà concluso), ci sarà tempo e modo di analizzare le singole modifiche e novità, nella forma definitiva che avranno assunto e magari ci sarà spazio anche per apprezzare alcune scelte come opportune e condivisibili, ma evidentemente non è questo il punto.

Il metodo che ha prodotto le scelte poi tradotte nelle proposte contenute nel DDL, ci fornisce infatti la conferma, non necessaria né richiesta ma certamente preoccupante, che anche di fronte a temi così essenziali, alla fatica richiesta della riprogettazione dei modelli, si preferisce la pigra opzione che si limita a reiterare l'illusione o, peggio, l'inganno affidato alle inesistenti virtù taumaturgiche degli 'amuleti penalistici' con i quali si adornano i provvedimenti legislativi.

---

[1] Il DDL è reperibile al link https://www.camera.it/leg19/126?tab=&leg=19&idDocumento=1717&sede=&tipo=