NOTA INFORMATIVA N.24/2022

Responsabilità dell'impresa e crimini informatici

1. Il reato informatico e responsabilità dell'impresa

L'analisi della criminalità informatica è sempre stata legata a due diversi approcci, che postulano premesse teoriche piuttosto lontane tra loro, e sembra debitrice all'intrinseca ambivalenza della nozione di reato informatico, amplificata dallo scorrere del tempo e dal mutare dei connotati e del ruolo degli strumenti tecnologici sui quali appunta la sua tutela.
Da un lato, infatti, vi sono reati informatici che sono tali in quanto commessi attraverso mezzi informatici o telematici (includendovi, oggi, anche i mobile devices); dall'altro, con la medesima locuzione ci si riferisce comunemente a reati che producano conseguenze, più o meno dannose, su dati, programmi, informazioni, files, etc.
Per l'effetto, secondo una prima prospettiva, si è inteso l'ambiente informatico come la mera riproduzione smaterializzata della vita reale o analogica. Così facendo, si è perpetuata l'idea che, in fondo, l'esigenza di tutela che si andava affermando potesse essere soddisfatta per il tramite di semplici clausole di estensione delle fattispecie incriminatrici già esistenti. Esemplifica questa prima tendenza l'introduzione dell'art. 491-bis c.p., nelle varie formulazioni che si sono succedute nel tempo: si tratta, com'è noto, di una disposizione caratterizzata da una tecnica normativa piuttosto infelice, peraltro foriera di non marginali incertezze applicative; acuitesi, da ultimo, con la depenalizzazione delle falsità in scrittura privata recata dal d.lgs. n. 7/2016. Ma c'è anche un diverso atteggiamento verso il settore informatico, che tende, al contrario, a rimarcarne la specialità, quasi a ogni costo. Ciò ha condotto al varo di nuove fattispecie, talora di dubbia consistenza criminologica e caratterizzate da una tipicizzazione non sempre soddisfacente. Si pensi, per esempio, agli artt. 635-bis e 635-quater c.p., nonché alle modifiche recentemente apportate

- dall'art. 19 legge n. 238/2021 (c.d. legge europea 2019-2020)
- agli artt. 615-quater e 615- quinquies e agli artt. 617-quater e
- 617-quinquies c.p., che, nel complesso, sono stati (ulteriormente) sbilanciati verso modelli di tutela ispirati al pericolo astratto, quando non al pericolo presunto.

Ma anche alla tipicizzazione della figura dell'operatore di sistema, in chiave aggravatrice, scollegata da ogni sostrato concreto effettivo. Ancora, si è dato vita a fattispecie che, al fondo, sembrano prive di una reale identità, e facilmente sussumibili nella più ampia cornice di altri reati (così, per esempio, la frode informatica).
Oggi occorre tener conto della vertiginosa progressione dello sviluppo del mezzo e dell'ambiente informatico. Difatti, il percorso evolutivo di questo sottosettore non è più relegato alla linearità dell'evoluzione tecnica, ma apre a scenari tanto ampi quanto frastagliati. L'informatica, intesa appunto come mezzo e come ambiente, taglia i più diversi settori disciplinari, interferendo col patrimonio, col diritto d'autore, con la privacy, con la disciplina dei marchi, dei brevetti e del segreto industriale, con la tutela dell'identità, col diritto del lavoro, con la valutazione delle scelte gestorie, etc.
Le considerazioni appena svolte, e i loro sviluppi, giocano un ruolo decisivo nell'analisi dell'impatto dei reati informatici sulla responsabilità da reato degli enti.
Com'è noto, i reati informatici che possono dar luogo alla responsabilità ex d.lgs. n. 231/2001 sono previsti all'art. 24 e all'art. 24-bis d.lgs. 231/2001, che richiama, pur diversificando la risposta sanzionatoria, una serie eterogenea di fattispecie. Si tratta, più nel dettaglio,

- dei delitti di lesione del domicilio informatico (artt. 615-ter e 615-quater c.p.);

- del delitto di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.);
- dei delitti di violazione della segretezza attraverso l'intercettazione, l'impedimento o l'interruzione di comunicazioni informatiche o telematiche, ovvero di installazione di apparecchiature idonee allo scopo (artt. 617-quater e 617- quinquies c.p.);
- dei delitti di danneggiamento informatico (artt. 635-bis, 635-ter, 635-quater e 635-quinquies c.p.);
- dei delitti di falso in atto pubblico informatico (art. 491-bis c.p.);
- del delitto di frode informatica del certificatore di servizi di firma elettronica (art. 640-quinquies c.p.);
- dei delitti che mettono a repentaglio la sicurezza delle reti e dei sistemi informatici delle amministrazioni pubbliche e degli enti da cui dipendano funzioni essenziali dello Stato (art. 1, commi 11 e 11-bis, d.l. n. 105/2019, conv. dalla legge n. 133/2019).

Questi ultimi sono previsti da una singola fattispecie a struttura sanzionatoria, la quale individua diverse ipotesi di reati propri e in un reato omissivo proprio, tutti ascrivibili unicamente ai soggetti, pubblici o privati, aventi sede nel territorio nazionale e che siano inclusi nel perimetro di sicurezza nazionale cibernetica, per come definito dalla relativa normazione extra-penale. La casistica classicamente richiamata con riguardo a una possibile responsabilità dell'ente per la commissione di un reato informatico è fin troppo nota perché sia il caso di attardarvisi: l'ente potrebbe giovarsi della produzione alla pubblica amministrazione di atti falsi, oppure potrebbe alterare o danneggiare gli stessi registri pubblici informatici allo scopo di far emergere condizioni di favore in realtà inesistenti, ovvero ancora danneggiare un concorrente o creare fondi neri attraverso artifici informatici.

2. Questioni problematiche

Nonostante l'importanza che palesa l'intersezione delle fattispecie in discorso con la corporate liability, la giurisprudenza sul punto è sostanzialmente inesistente. Ciò sembra riconducibile ad almeno un duplice ordine di fattori.

In prima battuta, e in via generale, è certamente decisiva la tutt'ora perdurante discontinuità nell'applicazione del d.lgs. n. 231/2001 da parte degli uffici di Procura, talora particolarmente attivi, talvolta restii, nella elevazione di addebiti agli enti collettivi (o nella loro archiviazione, rimessa, com'è noto, all'esclusivo giudizio dell'organo di accusa; art. 58). Peraltro, considerando il fatto che la maggior parte dei reati-presupposto in esame è di competenza distrettuale (art. 51, co. 3-quinquies, c.p.p.), la schiera dei decisori si riduce drasticamente, amplificando la condizione appena descritta.

In secondo luogo, le complessità regolarmente connesse all'individuazione dell'autore materiale dell'illecito penale si acuiscono particolarmente con riguardo alla commissione di un computer crime. Ciò sembra dipendere, a sua volta, da tre distinte condizioni.

Da un lato, la smaterializzazione che è consentanea a questo genere di illeciti lascia flebili tracce, comportando non sempre superabili difficoltà nella individuazione dell'autore materiale, anche in ragione delle difficoltà connesse all'assicurazione al processo di questo genere di prova in conformità agli standard sempre più elevati che si vanno affermando. Ciò, naturalmente, tende a minare in partenza la stessa possibilità di acquisire gli elementi in merito alla responsabilità di un soggetto apicale o subordinato; con tutto ciò che ne consegue, sul versante probatorio, con riferimento alla responsabilità dell'ente.

Dall'altro lato, la realtà quotidiana ci consegna una cultura dell'identificazione informatica che solo di recente si è avviata verso un cambiamento deciso nel segno di una maggiore affidabilità dei relativi strumenti di controllo. Le autenticazioni forti stanno rapidamente soppiantando il sistema di accreditamento tradizionale che si sostanzia nella semplice coppia di username e password, ma solo nelle realtà di maggior spessore, le uniche in grado di far fronte alla predisposizione di una simile dotazione informatica. Al contrario, il tessuto imprenditoriale, nella sua maggior parte, non articola la sua organizzazione con strumenti tecnologici avanzati e si caratterizza, non di rado, per la promiscuità nell'uso delle credenziali. Tuttavia, quand'anche si volesse mettere in pratica un sistema consimile, si aprirebbe lo scenario relativo alle difficoltà connesse al monitoraggio nell'impiego di credenziali, il quale,

specialmente là dove queste ultime siano ancorate a sistemi di autenticazione forte o biometrici, incontrerebbe gli ostacoli posti dall'intersezione delle guarentigie lavoristiche col diritto alla privacy.
Infine, un ultimo dato di sicura influenza riguarda l'intrinseca transnazionalità del reato informatico, soprattutto se mirato contro enti che abbiano server e piattaforme disseminate per il globo, ovvero si appoggino a organizzazioni ugualmente strutturate. Ciò apre tanto agli scenari del reato-presupposto commesso all'estero, espressamente tematizzati dall'art. 4 d.lgs. 231/2001, quanto a quelli, speculari, della responsabilità del soggetto giuridico estero per i reati commessi in Italia.
Tema, quest'ultimo, che divide profondamente la dottrina tra chi nega la punibilità di tali illeciti e chi invece ritiene decisivo il locus commissi delicti del reato-presupposto, valorizzando il carattere "derivato" della responsabilità alla luce del disposto dell'art. 36 d.lgs. n. 231/2001, ferma la sua autonomia, in considerazione della natura obbligatoria della legge italiana, indipendentemente dall'esistenza di fonti normative che regolino analogamente la materia nel paese di origine. Ancora, si fa leva sulla l. n. 146/2006 (e in particolare sull'art. 10), con la quale si è dato ratifica alla Convenzione contro il crimine internazionale delle Nazioni Unite, prevedendo anche ipotesi di responsabilità degli enti collettivi, la cui natura estera o nazionale non assumerebbe rilievo in seno all'art. 1.
La risoluzione dell'interrogativo è peraltro condizionata dalle diverse premesse teoriche da cui si muove nella ricostruzione dell'essenza stessa della responsabilità degli enti collettivi, che non può essere compiutamente ripresa nell'economia del presente contributo. È ben chiaro, però, che nelle impostazioni da ultimo ricordate trova implicito accoglimento la peculiare ricostruzione unitaria del reato e dell'illecito dell'ente in seno alla quale la colpa da organizzazione svolge una funzione sostanzialmente esimente (come fatto impeditivo), anziché costituire il centro dell'illecito, inteso come diversa e ulteriore forma di responsabilità originata (e condizionata) dal reato presupposto, che concorre a definire una fattispecie pluriascrittiva eventuale. V'è, poi, un terzo orientamento, secondo il quale i termini della questione possono ricomporsi avendo riguardo al fatto che l'ente non è l'autore del reato bensì della fattispecie dell'illecito amministrativo, di cui il primo costituisce un singolo elemento: da questo punto di vista, quindi, il locus commissi delicti non entra a far parte della fattispecie astratta mentre assumerebbe decisivo rilievo il luogo dell'esercizio dell'attività di impresa, tenendo in debito conto la disciplina extra-penale di riferimento, e in particolare il diritto internazionale privato (art. 25 l. n. 218/1995). Del resto, si osserva, altro è la giurisdizione, altro è l'individuazione dei destinatari della disciplina e dei presupposti sostanziali della responsabilità, la cui idoneità all'applicazione extraterritoriale è di tutt'altro che palmare evidenza, con l'effetto di rendere possibile un giudizio di equivalenza funzionale rispetto alle forme di compliance eventualmente previste nel Paese di origine.

3. L'interesse e il vantaggio dell'impresa

Le questioni poste trovano ulteriore complicazione là dove si coniughino al riscontro di un effettivo interesse per l'impresa, come richiesto dall'art. 5 d.lgs. n. 231/2001. In effetti, escluso, da un lato, che nell'ipotesi di concorso con soggetti estranei assuma rilevanza un interesse collegato unicamente all'agire di questi ultimi, ma non al reato in quanto tale, e assodata, dall'altro lato, la significatività di un interesse promanante tanto dall'agire dei soggetti intranei, quanto dal reato inteso nella sua complessità, occorre domandarsi cosa ne sia dei casi in cui l'interesse si colleghi a un reato commesso da terzi, ma non dipenda direttamente dal contributo concorsuale dell'intraneus. In tali casi, il riaffiorare di una proiezione soggettivistica del concetto, intesa quale finalità dell'agire, rischia di divenire il collante che tiene insieme l'ascrizione dell'illecito dell'ente alla mera prava voluntas dell'intraneus.
Ma se tanto può dirsi con riguardo al reato informatico inteso quale fine dell'agire criminoso, quid iuris con riguardo a un reato-mezzo, di per sé incapace di produrre un interesse/vantaggio, che sia tuttavia funzionale alla commissione di un reato fondativo della responsabilità dell'ente, e posto in essere nel suo interesse o a suo vantaggio? Si è detto che esiste una fenomenologia criminale che vede i soggetti interni all'ente quali mandanti del reato informatico-fine e delle difficoltà che emergono nel provare a fondare una responsabilità dell'impresa per un illecito sostanzialmente impossibile da impedire mediante la protocollazione delle attività. Ma vi sono anche altre ipotesi, in cui un reato-mezzo è

commesso all'interno dell'ente, intendendosi con ciò realizzato da soggetti intra- nei e nell'ambito dell'impresa.

La questione appena posta, a sua volta, lascia intravedere un ulteriore risvolto: occorre infatti comprendere se questa attività sia, di per sé, rivolta alla sovversione dei presidi di sicurezza informatici che tendono ad assicurare la compliance aziendale, ovvero se essa ricada al di fuori di queste, e quindi su sistemi che siano diversi o di altri interlocutori dell'ente o di suoi competitor. L'interrogativo che si pone riguarda l'eventuale attrazione di un reato-presupposto non produttivo di un diretto vantaggio nell'ambito della responsabilità dell'ente in forza della sua unificazione normativa nel segno del regime del reato continuato, che disciplinerebbe l'agito della persona fisica. In altri termini: là dove un reato informatico sia servente alla commissione di un reato fine, e entrambi siano appartenenti al c.d. catalogo 231, v'è da domandarsi se il primo possa essere ritenuto fondativo della responsabilità corporativa anche là dove non sia produttivo ex se di un interesse/vantaggio, ma solo nel suo combinarsi con il secondo.

Si tratta di uno scenario distinto dalla impiegabilità del concetto di interesse indiretto, praticato da una minoritaria giurisprudenza di merito, e centrato sul fatto che la percezione di vantaggi illeciti consentirebbe all'ente colpevole di poter essere più concorrenziale nel mercato di riferimento. Com'è stato efficacemente rilevato, così l'interesse si risolverebbe in una proiezione postuma di un vantaggio già percepito, alterando, con una surrettizia inversione, il criterio imputativo posto dall'art. 5.

Al contrario, la domanda di fondo è se sia concepibile in capo all'ente un macro-illecito composito retto da un interesse/vantaggio improprio, dipendente esclusivamente dalla commissione del reato-fine. Par superfluo ricordare, in proposito, che proprio la prova del collegamento rilevante tra persona fisica e giuridica è il perno fondamentale che consente di identificare l'ente-organizzazione come centro di imputazione del rischio-reato, in quanto protagonista della vita dell'impresa. A dire il vero, la questione sembra complicarsi notevolmente al divaricarsi dei contenuti assegnati alle nozioni dell'interesse e del vantaggio. Com'è noto, a mente della relazione al d.lgs. 231/2001 e di non pochi autori, tali requisiti dovrebbero intendersi come alternativi, incorrendosi altrimenti in una sostanziale i*nterpretatio abrogans* del concetto di vantaggio. Così inteso, l'art. 5 d.lgs. 231/2001 renderebbe possibile l'ascrizione dell'illecito indipendentemente dall'originaria finalizzazione all'interesse dell'ente là dove si giunga all'obiettiva acquisizione di un vantaggio, e viceversa. L'approdo interpretativo descritto sarebbe suffragabile anche avendo riguardo all'art. 12, co. 1, lett. a), là dove si prevede la riduzione della sanzione pecuniaria nel caso in cui il reato sia stato commesso nell'interesse esclusivo o prevalente di altri e l'ente non ne abbia ricavato vantaggio o ne abbia ricavato uno minimo. Questo orientamento è notoriamente fronteggiato da una diversa linea interpretativa, secondo la quale la formula interesse e vantaggio costituirebbe un'endiadi: tale conclusione dipenderebbe dalla valorizzazione dell'art. 5, ult. co., d.lgs. 231/2001, secondo il quale il collegamento tra ente e reato si spezzerebbe nel momento in cui si verifichi la totale assenza dell'interesse. Del resto, si osserva, la stessa impostazione della relazione di accompagnamento risulterebbe contraddittoria, trattando a un tempo i requisiti come alternativi e cumulativi, atteso che, in ogni caso, essa si tradurrebbe nell'interpretatio abrogans dell'ultimo comma dell'art. 5.

Un terzo orientamento, infine, si propone di mediare tra i due già descritti, affermando che il concetto di vantaggio, sebbene non alternativo tout court rispetto a quello di interesse, debba comunque mantenere un significato autonomo. Il criterio ascrittivo manterrebbe, dunque, una sua veste unitaria da apprezzarsi primariamente ex ante, al momento in cui il reato viene commesso. In questo senso, il vantaggio assumerebbe una valenza specificativa, segnalando che la nozione di interesse deve trasformarsi in una entità dalla obiettiva rilevabilità. Ferma la rilevanza oggettiva dell'interesse, ovverosia la sua idoneità causale a cagionare un beneficio per l'ente questo può intendersi sia quale criterio avente natura relazionale, richiedendo un nesso tra la condotta e la ricaduta favorevole (una qualità intrinseca della condotta), ovvero come criterio che richiede di contestualizzare l'agito nella prospettiva oggettivistico-funzionale dell'espletamento delle attività dell'ente, indipendentemente dalle sue caratteristiche intrinseche. Così, per valutare la sussistenza del requisito in parola occorrerebbe concentrare l'attenzione sul contesto in cui la condotta si colloca, dovendosi richiedere che essa si ponga nell'ambito di attività, di per sé lecite, compiute nell'interesse dell'ente. È noto altresì che sul fronte

giurisprudenziale manca un indirizzo davvero consolidato, anche se la giurisprudenza più recente sembra poggiarsi sull'orientamento intermedio sopra descritto, ribadendo l'alternatività tra i criteri ascrittivi. La giurisprudenza successiva ha poi precisato che l'accertamento di un interesse esclusivo dell'autore o di terzi vale a escludere la responsabilità dell'ente, tenuto conto che può ben ipotizzarsi un interesse prefigurato come discendente da un indebito arricchimento eventualmente non realizzato, e, invece, un vantaggio obiettivamente conseguito tramite la commissione di un reato; così come vi può essere un reato commesso nell'interesse dell'ente, che tuttavia è improduttivo di vantaggi.
Tuttavia, si osserva, la sussistenza del vantaggio potrebbe essere sufficiente a far aggallare la responsabilità dell'ente là dove non sia possibile accertare un effettivo interesse proprio dell'ente in prospettiva ex ante e contestualmente non sia accertata la sussistenza di un interesse esclusivo da parte di altri. Peraltro, occorre notare che la lettura giurisprudenziale dei concetti in esame è non di rado orientata dalla ricorrenza di reati presupposto di natura colposa che, come tali, comportano virate concettuali non sempre marginali. Proprio in relazione a tali fattispecie si è espressa una recente pronuncia della Suprema Corte, nella quale si è ribadito che l'interesse e il vantaggio devono essere intesi come alternativi e concorrenti tra loro, ritenendo che il primo si connetterebbe a una valutazione teleologica del reato, apprezzabile ex ante e secondo un metro di giudizio marcatamente soggettivo mentre il vantaggio avrebbe una connotazione essenzialmente oggettiva, come tale valutabile ex post, sulla base degli effetti concretamente derivati dalla realizzazione dell'illecito. L'interesse viene quindi ricostruito imperniandolo sulla consapevole e/o sistematica violazione delle norme prevenzionistiche che consenta riduzioni di costi o contenimenti di spesa, valutata secondo il criterio del bilanciamento: un interesse rilevante per l'ascrizione dell'illecito colposo all'ente sarebbe riscontrabile là dove l'omessa adozione delle cautele rappresenti l'esito di una scelta finalisticamente orientata a risparmiare sui costi di impresa. Quanto al vantaggio, la Corte osserva che è necessaria una rilevazione assai scrupolosa del beneficio perseguito o ritratto dall'ente, sottolineando che non ogni risparmio di spesa, pur eventualmente presente, può ipso facto costituire il fondamento dei criteri in esame.
Ferma l'opportunità di mantenere concettualmente distinte le due nozioni, la lettura soggettivistica dell'interesse, almeno in dottrina, risulta recessiva. Nondimeno, la questione posta resta essenzialmente appesa al diverso modularsi dell'interesse e al tipo di relazione che instaura col vantaggio. La deviazione verso una nozione soggettivistica dell'interesse, a cui apre la più recente giurisprudenza, sembra contigua allo scenario in cui esso possa essere ricostruito in chiave finalisticamente connessa alla commissione del reato-fine, che consenta la realizzazione di un complessivo vantaggio. Diversamente, la rivendicazione di una concezione obiettiva di interesse disinnesca questa linea interpretativa, in cui la responsabilità dell'ente rischia di tradursi in una mera appendice di quella individuale. In questa prospettiva, sembra emergere chiaramente l'assenza, in relazione al reato-mezzo, di un precipuo e autentico interesse che ne segni l'appartenenza anche all'ente. Occorre infatti guardarsi dalla tentazione di traslare in questo sistema normativo i canoni ascrittivi tipici della responsabilità della persona fisica. Il reato continuato trova ragione, peraltro in chiave di favore, nella mitigazione della risposta sanzionatoria là dove il reo abbia deliberato l'azione criminale in un'unica soluzione, così dimostrando un minor tasso di colpevolezza. Diversamente, polarizzare il fuoco dell'interesse/vantaggio dell'ente unicamente sul reato-fine, attraendovi anche il reato-mezzo, finirebbe non con l'aggregare entità giuridiche già esistenti bensì col fondare la stessa ascrivibilà all'ente di una fatti- specie che, in difetto del compimento della seconda, resterebbe inevitabilmente insuscettibile di condurre all'integrazione dell'illecito.

4. Crimini informatici finalizzati alla elusione del modello: l'impresa vittima di se stessa

Resta, infine, un'ultima fenomenologia criminale da prendere in esame, relati- va alla commissione di un reato-mezzo informatico su sistemi informatici propri dell'ente, con lo scopo di aggirare i meccanismi di controllo attuati in aderenza al modello di gestione del rischio reato.
Si tratta di uno scenario che merita qualche ulteriore chiarimento preliminare. Come si è notato in apertura, l'apporto dell'informatica all'interno dell'impresa sta mutando rapidamente: non solo sotto il

profilo quantitativo ma soprattutto sotto il profilo qualitativo. Il c.d. web3, altamente decentralizzato e basato su reti crittografate in blockchain, dietro le quinte sta già prendendo il posto della rete che conosciamo, ma presto comincerà a mostrarsi anche all'utente medio. Siamo poi prossimi al varo del Metaverso, autentico oltre-mondo collaborativo e immersivo nel quale, sebbene parzialmente, sarà sovvertito lo snodo centrale che ha sempre distinto il mondo reale da quello digitale, ovverosia la sua infinita replicabilità e l'indeterminatezza degli spazi a esso connessi (il riferimento è soprattutto ai cc.dd. NFT, Non Fungible Token). L'assicurazione di una dimensione certa e immodificabile ai prodotti puramente informatici e alla loro paternità, infatti, sembra condurre a una metamorfosi profonda del sistema imprenditoriale, oramai avviato verso il consolidamento della c.d. industria 4.0, i cui complessi risvolti giuridici non sembrano del tutto predeterminabili ex ante. Anche in questo frangente, le novità che si annunciano comportano la necessità di una riflessione aggiornata nelle sue fondamenta. Per quanto qui interessa, occorre muovere dalla considerazione che la sfida della modellistica in tema di responsabilità dell'ente è stata legata, fin dalla sua istituzione, alla capacità di incanalare il comportamento dei soggetti entro procedure definite da specifici protocolli, poi replicati in strumenti informatici altamente esposti a una manipolazione interna.

Tuttavia, è un punto incontroverso che ciò che rileva sia più la predisposizione del mezzo, che l'impedimento dell'esito. Del resto, la natura normativa del rimprovero colposo che viene rivolto all'ente in debito di organizzazione non può che avere natura modale, riportando l'interprete alla necessità di leggere protocolli e controlli in valore assoluto, al netto della loro effettività nel singolo caso concreto. In altri termini, mutuando gli approdi interpretativi più recenti in tema di colpa penale, il giudice non dovrebbe mai creare ex post la cautela doverosa che si sarebbe dovuta predisporre, alla stregua di un apriorismo rispetto al sapere tecnico preesistente. La sanzione per l'ente, in effetti, non sembra connessa unicamente al fatto che si è verificato, quanto, e soprattutto, al difetto strutturale che ne ha consentito la realizzazione. Da questo punto di vista, ciò che consente la generalizzazione e la massificazione di strumenti di assicurazione della immodificabilità delle procedure, oggi riservati a importanti realtà imprenditoriali, è proprio l'impiego di tecnologie informatiche garantite, entro cui l'operatore non possa muoversi del tutto liberamente, ma essere, al contrario, accompagnato nel percorso virtuoso immaginato dal compilatore del modello di gestione.

L'impiego della tecnologia blockchain e delle intelligenze artificiali, specialmente collegate ai big data, aprono a nuovi scenari in grado di stringere i controlli aziendali consentendo la rilevazione di segnali di allarme di vario o di violazioni della normativa antiriciclaggio, ovvero ancora in tema di privacy. Com'è noto, la blockchain è definibile come un database per la gestione di transazioni crittografate su una rete decentralizzata di tipo peer-to-peer, nel quale i partecipanti alla rete verificano, approvano e registrano tutti i blocchi con i dati di ciascuna operazione, riportandone la verifica su ogni singolo nodo. Per l'effetto, ogni informazione registrata è simultaneamente presente su tutti i nodi della rete, e diventa quindi immodificabile, salva l'approvazione della rettifica da parte della maggioranza dei nodi, che in ogni caso si aggiungerà in coda alla precedente informazione. Lo stratificarsi delle informazioni, in altri termini, non avviene mediante la sovrascrittura ma attraverso un sistema di glossatura che è presidiato da puzzle crittografati di enorme complessità. In breve: ogni operazione viene aggiunta alla catena delle registrazioni conservata nell'archivio, decentralizzato e frammentato in tutti i nodi, che nel loro continuo dialogo confrontano continuamente le varie copie, sostituendo le eventuali anomalie con delle versioni corrette.

È per questa decisiva ragione che è impossibile, all'atto pratico, sovvertire i contenuti di una registrazione inserita nel registro condiviso e, dall'altro lato, la gestione dei flussi è resa trasparente e perfettamente storica: non è, infatti, possibile eliminare vecchie informazioni, ma solo aggiungerne di nuove. Tali tecnologie, per quanto qui interessa, possono essere impiegate per istituire una connessione

automatizzata tra il modello di organizzazione e gestione del rischio-reato e, per esempio, le procedure anticorruzione e antiriciclaggio nonché con i sistemi di gestione aziendale di tracciamento del denaro o delle merci. Un database distribuito e crittografato, con le garanzie di sicurezza e trasparenza sopra sommariamente descritte, potrebbe essere la chiave di volta del consolidamento di una compliance effettiva, impedendo una larga parte dei reati che, a oggi, costituiscono il presupposto della responsabilità degli enti collettivi. D'altra parte, un controllo decentralizzato è senz'altro la miglior garanzia di efficacia e tendenziale incorruttibilità, rendendo l'efficacia del medesimo condivisa da tutti gli operatori.

È un approccio che tende verso i confini del c.d. *legal Protection by design*, applicato alle piattaforme informatiche dell'ente e dipendente dall'impiego di strumenti preventivi di contrasto alla elusione dei protocolli operativi. Esigenza, peraltro, già avvertita chiaramente dalla prassi e della riflessione dottrinale, che non manca di rilevare il preoccupante tasso di disinteresse che caratterizza la produzione giurisprudenziale che si misura con le scelte operate in sede prevenzionale, sia su base esperienziale che tecnico-specialistica (salva la presunzione di conformità prevista dall'art. 30, comma 5, d.lgs. 81/2008).

In questo senso, il ricorso a protocolli operativi che, giovandosi dell'apporto informatico, possano influenzare il comportamento dei soggetti determinando esiti predefiniti è una prospettiva di sicuro interesse nella lettura della responsabilità degli enti collettivi. In simili contesti, sarebbe l'ambiente informatico a condurre l'operatore entro binari certi, frutto di una elaborazione tecnica che modella il luogo di lavoro informatico secondo le procedure e i meccanismi di controllo propri del modello di organizzazione e gestione del rischio-reato, facendo sfumare, sino a scomparire, la distinzione tra regole giuridiche e regole tecniche di sistema. Così, la criminalità informatica sembra trovare nuovi scenari di applicazione proprio all'interno dell'ente collettivo, dove il progressivo prendere piede di questo genere di tecnologie porterà, prima o poi, all'emersione di una fenomenologia illecita che si proponga lo scopo di superare quelle barriere che si frappongono alla possibilità di ipotizzare un interesse o di conseguire un vantaggio. Ne deriva la possibilità che l'oggetto del reato informatico cessi di essere un sistema altrui, e divenga invece la stessa struttura dell'ente coinvolto, in quanto primo argine alla possibilità di realizzare o di occultare la commissione di un reato-fine. In positivo, lo scenario descritto si presenta in questi termini: presidiare le procedure messe a punto con sistemi informatici automatizzati che garantiscono la perfetta tracciabilità delle azioni aiuta a isolare l'elusione fraudolenta del modello di gestione. D'altra parte, però, si palesa un'autentica contraddizione in termini: l'ente, a un tempo, potrebbe essere autore e vittima del medesimo reato-presupposto. Da un lato, infatti, esso sarebbe attuato in vista di un (futuribile) interesse o vantaggio, pur con la compromissione di sistemi il cui ripristino, in via immediata, comporta inevitabilmente un danno economico. Dall'altro lato, però, il reato-mezzo informatico sarebbe reso necessario proprio dalla predisposizione di procedure e automatismi informatici che siano in grado di contenere l'attività dei soggetti intranei entro il perimetro della legalità. È, questo, un conflitto che potrebbe aprirsi tra la valenza del criterio oggettivo dell'interesse/vantaggio e quello soggettivo della colpa da organizzazione, la cui insussistenza si manifesterebbe in re ipsa.

3 maggio 2022

Avv. Bruna Capparelli