minimizzazione. Il report, in particolare, sottolinea la necessità di soddisfare le seguenti proprietà: i dati per la diagnosi e il trattamento dei singoli pazienti devono essere identificabili; quelli per la ricerca medica (eventualmente trattati su larga scala) devono essere adeguatamente pseudonimizzati per garantire che il livello di probabilità di re-identificazione sia ridotto al minimo; deve essere infine presente la capacità di gestire più fonti di dati del paziente, compresi i dispositivi indossabili e le app.

Uno dei case study riportati nel report esplora la situazione di un dispositivo indossabile per il monitoraggio continuo del glucosio (CSM) che, al contempo, monitora anche la pressione sanguigna, i livelli di caffeina e i livelli di lattato 7. Il dispositivo carica i flussi di dati raccolti nel cloud per l'archiviazione e l'ulteriore elaborazione da parte dell'utente stesso e di soggetti terzi, come la sua famiglia e i medici. La complessità principale da superare è quella di permettere all'utente di selezionare specifici flussi di dati da condividere con soggetti specifici e l'ora e il tempo d'accesso, per esempio permettere a un soggetto terzo l'accesso ai dati corrispondenti agli ultimi tre mesi per specifici set di dati. In tal senso, sono descritte alcune soluzioni crittografiche per proteggere la privacy dei dati sanitari durante la loro condivisione tra utenti diversi. In particolare, si tratta di tre tecniche di crittografia asimmetrica: con chiave pubblica, l'Attribute Based Encryption (ABE) e la Proxy Re-encryption. La tecnologia con chiave pubblica prevede che ogni segmento di dati da condividere venga crittografato dall'utente con la chiave pubblica del destinatario interessato. Tale soluzione, tuttavia, risulta poco pratica quando i dati devono essere condivisi tra più entità. L' ABE comporta invece la crittografia dei dati con una chiave pubblica ABE, che consente l'esistenza di più chiavi di decifrazione legate a informazioni aggiuntive relative ai dati, chiamate attributi. La Proxy Re-encryption, infine, consente la condivisione di dati già criptati da una chiave pubblica a un'altra, senza che il proxy abbia accesso al set di dati non criptati.

Uno scenario tipico di condivisione di dati sanitari è quello della gestione delle cartelle cliniche elettroniche (EHR) da parte degli operatori sanitari. Sono cartelle che raccolgono la storia clinica del paziente e di solito vengono conservate in archivi centrali nazionali. Gli utenti possono autorizzare l'accesso ai propri dati ai medici curanti o alle istituzioni mediche. A seguito della pandemia, si è resa urgente la necessità di progetti di raccolta dati ai fini della progressione della ricerca scientifica e della prognosi. Di solito, essendo il sistema centralizzato, la gestione dei meccanismi di controllo degli accessi viene effettuata dal centro medico, affinché solo i fornitori di servizi sanitari autorizzati abbiano accesso alle informazioni personalizzate. Quando i dati devono essere trasmessi a ricercatori interni o esterni, occorre adottare misure di pseudonimizzazione, al fine di scongiurare l'identificazione del paziente.

ENISA, dunque, propone l'utilizzo della crittografia polimorfica e pseudonimizzazione (PEP), tecnologia che consente di crittografare i dati senza la necessità di stabilire in anticipo chi può decifrarli. Ciò significa che l'accesso ai dati può essere concesso successivamente, a diverse parti con chiavi differenti. Ad ogni individuo viene assegnato uno pseudonimo diverso per ogni richiesta di accesso, quindi ogni paziente ha un identificatore univoco. Questo identificativo viene trasformato in diversi pseudonimi a seconda del destinatario e del contesto della condivisione dei dati. Gli pseudonimi utilizzati per lo stesso paziente non possono essere collegati, preservando così la riservatezza dei dati del paziente. La PEP è già stata testata con successo in uno studio sul morbo di Parkinson e come proposta per il sistema olandese di Electronic Identification (eID).

In conclusione, la condivisione dei dati è un'opportunità di sviluppo notevole per il settore sanitario e per la società in generale, ma deve essere regolamentata adeguatamente per garantire la protezione dei dati personali e la fiducia degli individui e delle organizzazioni. In merito, "l'ingegneria della protezione dei dati" si rivela essere una grande alleata per rispettare i principi di privacy *by design* e *by default* previsti dall'art. 25 GDPR.

CARMINE ANDREA TROVATO

https://www.enisa.europa.eu/publications/engineering-personal-data-sharing

16. Il *working paper* dell'ISDA del gennaio 2023 sull'insolvenza nei mercati degli assets digitali

Nel gennaio 2023 l'International Swaps and Derivatives Association ("**ISDA**") ha pubblicato un *working paper* intitolato "*Navigating Bankruptcy in Digital Asset Markets: Netting and Collateral Enforceability*" vertente sui contratti derivati inerenti ai *digital assets*.

Il documento tra origine dai recenti fallimenti di FTX - nota piattaforma di *trading online* -, "TerraUSD" - una *stablecoin* -, "Three Arrows

Capital" – *hedge fund* specializzato in criptovalute - , "Celsius" - una società attiva nel segmento *crypto lender* – e alla richiesta ai sensi del Chapter 11 di "BlockFi" – altra impresa di *crypto lender*.

I suddetti eventi hanno scosso il mercato e incrinato la fiducia degli investitori (*rectius*, risparmiatori) imponendo alle Autorità di supervisione del mercato di approntare rapidamente un quadro regolatorio adeguato.

Tale disciplina deve anche tenere conto delle peculiarità del fenomeno considerato. Per tale motivo, è difficile rispondere univocamente ad alcuni interrogativi. Ad esempio, come si individua il proprietario di un *digital asset*? E ancora, come si gestisce il rischio di credito di controparte in caso di insolvenza del gestore della piattaforma di *trading* o della *stablecoin*?

Il documento dell'ISDA si propone di rispondere a tale ultimo interrogativo analizzando due istituti: il "*close-out netting*" e i collaterali.

Preliminarmente, va detto che gli attori del mercato dovrebbero avere una chiara comprensione dei diritti e obblighi nascenti da rapporti contrattuali con oggetto *digital assets*.

Occorre, quindi, tentare di definire la natura giuridica degli *assets* digitali, la quale risente delle loro particolari caratteristiche giuridiche, tecnologiche ed economiche, nonché i connessi diritti e doveri.

Ebbene, il *working paper* si concentra sugli *assets* che utilizzano la *Distributed Ledger Technology* (c.d. DLT) in cui il bene non è controllato da un'entità centralizzata, ma la titolarità risulta distribuita tra i vari nodi della rete. A ciò si aggiunga che alcuni *asset* digitali esistono solo nella rete (ad esempio, i Bitcoin), poiché non configurano una rappresentazione digitale di un bene esistente nella realtà, altri rappresentano un fascio di situazioni giuridiche che esistono sia *online*, sia *offline*. Altri ancora esistono *online*, ma sono collegati con altri beni esistenti in natura, un sottostante.

Da quanto detto, emerge la difficoltà di coniugare tale fenomeno con gli attuali *legal frameworks*, che peraltro verosimilmente non conoscono la proprietà diffusa di un bene. Di conseguenza, il *paper* utilizza il termine "*holder*" in modo generico riferendosi a colui che ha il potere di controllare l'*asset* digitale e non come sinonimo di "*possessed*".

In merito alla gestione del rischio di controparte, il *close-out netting* è un istituto ampiamente diffuso nei contratti derivati per cui in caso di *termination* del contratto, ad esempio per insolvenza di una parte, tutte le obbligazioni originanti dal rapporto giuridico sono risolte, le prestazioni ad esse collegate sono valutate e tramutate nel pagamento di una somma (*lump sum*) dal debitore al creditore. Si tratta di un meccanismo che consente: i) la risoluzione anticipata di un accordo; ii) la valutazione delle prestazioni ancora dovute; iii) il pagamento di una somma in sostituzione delle varie prestazioni potenzialmente da eseguire; ma soprattutto, iv) di evitare che la *defaulting party* possa continuare a assumere diritti e obblighi seppur non sia più in grado di adempiervi regolarmente.

Il funzionamento di tale meccanismo, previsto dal modello contrattuale dell'*ISDA Master Agreement*, non cambia laddove il contratto abbia ad oggetto *digital assets*. È possibile, tuttavia, che alcuni ordinamenti giuridici non conoscano tale istituto. Esso, infatti, è sicuramente applicabile alle transazioni regolate dalla legge inglese e americana, ma non a quelle rette dal diritto degli stati europei che hanno attuato la dir. 2002/47/CE, c.d. *Financial Collateral Directive*. A ciò si aggiunga che la normativa secondaria emanata dalle Autorità di supervisione bancaria può determinare l'inoperatività del sistema di *close-out netting*.

Per tali motivi, il *paper* dichiara che l'ISDA sta lavorando per far includere il *close-out netting* in tutte le transazioni con oggetto un *digital asset*.

I collaterali, invece, sono beni dati in garanzia da un contraente ("*collateral provider*") all'altro ("*collateral taker*") al fine di mitigare l'esposizione al rischio di credito di controparte. In un contratto ciascuna parte può sia rilasciare che ricevere collaterali.

I benefici associati al rilascio di una garanzia sono diversi. Innanzitutto, i tempi per l'escussione sono generalmente brevi per gli *assets* liquidi. Addirittura, se i *collateral* sono *asset* digitali, l'incasso può avvenire quasi istantaneamente (c.d. "*atomic settlement*"). In secondo luogo, il collaterale esce dal controllo del garante.

In caso di *default* della parte che ha rilasciato la garanzia, l'altra può i) acquisire la proprietà del bene soddisfacendosi sino alla concorrenza dell'importo dovuto in base al contratto non adempiuto e restituendo l'ammontare della garanzia in eccesso (c.d. "*title transfer agreement*"); ii) acquisire un "*secondary proprietary interest*" sul collaterale e, di conseguenza, soddisfarsi sul bene (c.d. "*security interest*").

Per completezza, comunque, va detto che al trasferimento della proprietà del collaterale può seguire l'appropriazione del bene o l'esecuzione forzata, ossia la sua vendita con soddisfacimento sul ricavato.

La costituzione di una garanzia impone di interrogarsi su come determinare la proprietà di un *digital asset*. Il paper in commento, rinviando all'"*ISDA Legal Guidelines for Smart Derivatives Contracts – Collateral*", rileva che non esiste una risposta univoca in considerazione delle differenze tra i vari ordinamenti giuridici e che ogni considerazione al riguardo è influenzata da fattori tecnologici.

È necessario, inoltre, indagare come si perfeziona la garanzia avente ad oggetto i *digital assets*. Al riguardo, il *working paper* qui analizzato precisa che è difficile determinarlo a priori, a causa delle differenze tra gli ordinamenti giuridici, soprattutto sui concetti di "*control*" e "*possession*". Ad ogni modo, laddove un individuo possa dimostrare di avere il controllo su un *digital asset*, ad esempio perché quest'ultimo è stato trasferito in un suo *account* o *wallet*, è ragionevole supporre che la garanzia si sia perfezionata.

Assai condivisibilmente, il *paper* in commento, rinviando all' *ISDA Whitepaper* "*Contractual Standards for Digital Asset Derivatives*", evidenzia pure che le peculiarità degli *asset* digitali e degli ordinamenti giuridici coinvolti si riflettono, tra l'altro, nella formulazione dei contratti che li riguardano e nei conflitti di legge nascenti dai suddetti contratti.

Per concludere, il *working paper* dell'ISDA rileva che la rapida evoluzione del mercato e alcuni recenti accadimenti rendono sempre più importante sviluppare un quadro normativo armonizzato e chiaro riguardo ai derivanti inerenti ai *digital assets*.

EMANUELE STABILE

https://www.isda.org/2023/01/26/navigating-bankruptcy-in-digital-asset-markets-netting-and-collateral-enforceability/

17. La determina dell'Agenzia per la cybersicurezza nazionale del 3.1.2023 sulla tassonomia degli incidenti informatici da notificare

Il 3 gennaio 2023 è stata pubblicata sulla Gazzetta Ufficiale la determina (da ora anche la "**Determina**") dell'Agenzia per la cybersicurezza nazionale (da ora anche l'"**Agenzia**") recante la definizione degli incidenti ICT che devono essere notificati all'Agenzia.

La Determina è stata emanata in attuazione dell'art. 1, comma 3 bis D. L. 105/2019 (da ora il "**Decreto**"), convertito in L. n. 133/2019, recante "*disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale*".

La Determina si propone proprio di definire la tassonomia degli incidenti che possono avere un impatto negativo sulla rete, sui sistemi informativi e sui servizi informatici diversi dai "beni ICT" che i soggetti di cui all'art. 1, comma 2 bis del Decreto (c.d. "soggetti inclusi nel perimetro") sono tenuti a notificare.

L'art. 1 della Determina contiene le seguenti definizioni:

- "soggetto incluso nel perimetro", i soggetti di cui all'art. 1, co. 2 bis Decreto, ossia "*amministrazioni pubbliche, enti e operatori pubblici e privati di cui al comma 1 aventi una sede nel territorio nazionale, inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti dal presente articolo*";
- "*bene ICT*", ossia "*un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'art. 1, comma 2, lettera b)*" del Decreto;
- "*incidente"* indica *"ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici*";
- "*impatto sul bene ICT",* ossia la *"limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali*".

L'art. 2 della Determina definisce l'oggetto del provvedimento in esame, sostanzialmente coincidente con quanto sopra detto.

L'art. 3, infine, rinvia all'Allegato A alla Determina che si presenta diviso in due parti per la definizione della tassonomia degli incidenti. Nella prima sono elencati gli incidenti da notificare. Nella seconda, invece, sono descritti gli eventi da cui originano gli incidenti che dovranno essere segnalati.

EMANUELE STABILE

https://www.acn.gov.it/notizie/contenuti/si-rafforza-il-perimetro-nazionale-di-sicurezza-cibernetica