SISTEMA PENALE

FASCICOLO 6/2022

ISSN 2704-8098

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale.
Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2022, p. 5 ss.

INDICE DEI CONTRIBUTI

SISTEMA PENALE

6/2022

L'UTILIZZO CRIMINOGENO DELLA *BLOCKCHAIN*: GLI *SMART CONTRACT*

di Giovanni Paolo Accinni

SOMMARIO: 1. Gli *smart contract*: cenni introduttivi. – 2. Le caratteristiche criminogene degli *smart contract*. – 3. I c.d. "*criminal smart contract*". – 4. Il sistema *blockchain* nella concreta (in)operatività del diritto penale. – 5. L'astratta (ir)responsabilità concorsuale dello sviluppatore dello *smart contract*. – 6. Profili di applicabilità degli artt. 615-*quater* e 615-*quinquies* c.p. – 7. Conclusioni: il progresso tecnologico tra auto responsabilizzazione e minaccia di pena.

1. Gli *smart contract*: cenni introduttivi

Nell'ultimo decennio il ruolo di internet e del cyberspazio è diventato prepotentemente pregnante nella vita quotidiana di ciascun individuo: la maggior parte degli scambi, dei servizi e delle funzionalità precedentemente condotta nel mondo "fisico" è ora svolta nel mondo virtuale. Una delle innovazioni più *in auge* è certamente rappresentata in questi ultimissimi anni dalla c.d. *blockchain* (letteralmente "catena di blocchi")[1], che sta alla base del funzionamento delle c.d. criptovalute, ma che ha avuto poi sviluppi nei campi più diversi quali (ad esempio) la medicina. Con il generale

[1] La *blockchain* è un registro distribuito e decentralizzato (*Distributed Ledger Technlology* o *DLT*), caratterizzato dalla trasparenza e dalla tendenziale immutabilità e irrepudiabilità, che sfrutta la crittografia asimmetrica per la protezione e l'autenticazione delle transazioni (attraverso chiavi pubbliche e private) che sono iscritte e conservate in blocchi collegati tra loro cronologicamente. Si tratta di un sistema decentralizzato in quanto non vede la partecipazione di alcuna autorità centrale che certifichi e garantisca la veridicità delle transazioni. Pertanto, mentre in un sistema centralizzato la fiducia dei partecipanti è riposta nell'ente centrale che lo gestisce o lo supervisiona, in un sistema decentralizzato e distribuito la fiducia è nell'infrastruttura in sé, composta da tutti i partecipanti della rete (i nodi, organizzati secondo l'architettura della rete *peer to peer* o P2P47), secondo il principio del consenso ed il meccanismo delle ricompense (*proof of work*). Una copia dell'intero *ledger* è inoltre conservata a cura di ogni singolo nodo della rete, ed è accessibile da ognuno di essi, rendendo la *blockchain* trasparente e verificabile. Si differenzia quindi dai comuni *database* centralizzati in quanto i dati non sono conservati in uno (o più) *server*, dove tra i partecipanti alla rete vi è un rapporto *client-server*, ma ogni nodo è in posizione paritaria l'uno con l'altro. Ciò comporta anche una maggiore sicurezza del sistema in quanto l'attacco ad un singolo nodo non comprometterà il funzionamento né l'integrità dei dati. Un'altra caratteristica della *blockchain* è la "*scarsità digitale*" che permette di far assumere valore economico e di scambio a ciò che viene registrato sui registri distribuiti. I comuni documenti informatici possono invero essere copiati e duplicati senza particolare difficoltà infinite volte rendendoli indistinguibili l'uno dall'altro; l'uso della crittografia rende invece ogni transazione unica e quindi non duplicabile, conferendo così "scarsità" e perciò valore a tutto quanto il che viene trascritto sulla *blockchain*.

sviluppo della c.d. *blockchain* si è assistito però anche al contestuale approfondimento delle possibili devianze criminogene di siffatta tecnologia. La *blockchain* consente infatti di concludere transazioni *online* senza che vi sia bisogno di intermediari e (soprattutto) offre transazioni istantanee ed anonime tra individui. Ai vantaggi si contrappone così l'incoraggiamento dello sviluppo criminogeno del settore[2], concretizzatosi nell'immissione di *ransomware,* nel riciclaggio di denaro proveniente da attività illecite e nel commercio di beni illegali[3].

Le più evolute versioni della *blockchain*, come quella gestita dalla *community* Ethereum, hanno nondimeno iniziato ad offrire ulteriori funzionalità virtuose rispetto a quelle del mero trasferimento di valuta virtuale. Ci si riferisce in specifico alla possibilità di implementare l'uso dei c.d. *smart contract*[4]: un sostantivo con cui si identificano contratti ad esecuzione automatica, ossia che agiscono in modo autonomo secondo le condizioni prestabilite dalle parti e poi tradotte in un codice informatico. In particolare, l'esecuzione del contratto comporta tipicamente un trasferimento di criptovaluta a fronte dell'esecuzione della prestazione dedotta in obbligazione. Una volta verificato ed iscritto nella *blockchain* esso diviene quindi sostanzialmente irreversibile, riducendo perciò il rischio di un possibile inadempimento da parte dei "sottoscrittori"[5].

Un esempio di siffatta tecnologia è costituito dagli *smart contract* utilizzati dalle compagnie aree per gestire i rimborsi in caso di ritardi dei voli. Il riferimento è al caso di un passeggero che acquisti il proprio biglietto tramite l'applicazione di una compagnia che utilizzi la *blockchain* di Ethereum e che abbia creato uno *smart contract* per la gestione dei rimborsi. Lo *smart contract* prevede segnatamente che, se l'areo accumuli un certo ritardo, al passeggero venga riconosciuto un rimborso pari al 15% del prezzo corrisposto.

Ebbene, laddove in un sistema tradizionale la verifica del ritardo accumulato dall'aereo, della sussistenza delle condizioni per l'ottenimento del rimborso e la stessa esecuzione del pagamento richiederebbero (e richiedono) l'intervento di numerosi intermediari, necessitando di tempo e rimanendo subordinati alle valutazioni (ed alla buona fede) dei soggetti coinvolti nel processo, nel caso di utilizzo di uno *smart contract* ciò non è più necessario. Allorquando allo *smart contract* venga trasmesso il segnale automatico del ritardo accumulato dall'areo, il contratto provvederà a verificare in modo autonomo se quest'ultimo superi (o meno) la soglia a cui viene subordinata l'erogazione del rimborso e provvederà poi (altrettanto autonomamente) al rimborso di quanto dovuto al passeggero.

---

[2] A. JUELS, A. KOSBA, E. SHI, *The ring of gyges: Using smart contracts for crime*, in *aries* 40, 2015, 54.

[3] Si veda ad esempio il mercato sviluppatosi nel *dark web* denominato "via della seta" dove poteva ritrovarsi qualsiasi tipo di bene illegale. Cfr. sul punto: N. CHRISTIN, *Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace*, in https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf.

[4] Una delle criptovalute appositamente concepita per essere utilizzata per l'esecuzione degli *smart contracts* è *Ether*, implementata sulla piattaforma *Ethereum* ed attualmente la più utilizzata dopo il *Bitcoin*.

[5] L. BRUNONI, O. BEAUDET-LABRECQUE, *Smart contracts and cybercrime: a game changer?*, in *Математические структуры и моделирование* 4, 44, 2017, pp. 136-140.

Manifesto come si tratti quindi di una tecnologia foriera di nuovi impatti sul sistema giuridico odierno. In un ambiente commerciale tradizionale l'esecuzione dell'accordo dipende infatti dalla buona fede delle parti e, in caso di inadempimento, può essere fatto rispettare solo rivolgendosi al potere giurisdizionale. Di contro, gli *smart contract* eseguono automaticamente la prestazione tradotta nel codice informatico, eliminando perciò (da un lato) la necessità di fidarsi della controparte e (dall'altro) di dipendere da quest'ultima o dalle Autorità statali, una volta che i termini del sinallagma siano stati concordati e caricati sulla *blockchain*[6].

Eliminando il "problema" della buona fede contrattuale gli *smart contract* sono così destinati ad apportare sicuri benefici agli scambi commerciali. La crittografia e l'anonimità delle transazioni, tipiche del sistema *blockchain*, possono poi però essere utilizzate altresì per occultare il contenuto delle prestazioni dedotte negli *smart contract* e la stessa identità delle parti contraenti, esacerbando così il rischio che siffatti contratti possano essere utilizzati per la commissione di reati.

Per vero, l'analisi delle possibili implicazioni criminogene degli *smart contract* diviene tanto più interessante a considerarsi che (già oggi) gli stessi vengono utilizzati per scambiare ingenti quantità di valuta virtuale. Lo *smart contract* di valore più elevato ad oggi esistente sulla *blockchain* Ethereum ammonta (ad esempio) a circa 1.800 ETH[7], ossia ad un controvalore (in valuta *fiat*) pari (addirittura) a 400 milioni di dollari[8]. Insomma, una tecnologia che, se non opportunamente presidiata, potrebbe consentire operazioni illecite di significativa rilevanza economica e di altrettanto sicuro allarme sociale.

2. Le caratteristiche criminogene degli *smart contract*.

In via di prima approssimazione vi è che gli *smart contract* sono dotati di caratteristiche che li rendono intrinsecamente molto "appetibili" per il mondo criminale. La prima è (come detto) senz'altro l'anonimato, che deriva dal fatto che gli *smart contract* vengono implementati nel sistema *blockchain*. Come noto nella *blockchain* la tracciabilità delle singole operazioni non giunge infatti sino al punto di consentire di risalire alla reale identità degli operatori. In ciascuna operazione ogni *user* è identificato da una chiave pubblica ed una privata. Allorquando si effettui l'operazione, la *blockchain* registra la chiave pubblica del suo autore, mentre la chiave privata (la *password*) non viene pubblicata, ma rimane nell'esclusiva disponibilità del titolare. Ciò fa sì che quanto risulterà visibile pubblicamente non sarà mai il reale nominativo dell'utente, ma un mero numero identificativo corrispondente alla chiave pubblica del soggetto. Nel caso in cui un utente della *blockchain* vi distribuisca (*deploy*) uno *smart contract*, la relativa

[6] L. BRUNONI, O. BEAUDET-LABRECQUE, cit, pp. 136-140.
[7] M. NDIAYE, P.K. KONATE, *Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain*, in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*, IEEE, p. 2.
[8] T. CHEN et al, *A generic online detection framework for smart contracts*, in *Proceedings of the 27th Network and Distributed System Security Symposium*, 2020.

distribuzione rimarrà perciò riconducibile alla sola chiave pubblica dell'utente, ma non sarà (appunto) possibile comprendere la reale identità fisica delle parti del contratto[9].

La seconda caratteristica sta nel fatto che siffatti strumenti eliminano qualunque alea soggettiva intesa all'attuazione del contratto nel senso che la corretta esecuzione della prestazione è indipendente dalla buona fede delle parti ed avviene in via "automatica" al solo verificarsi delle condizioni prestabilite nello *smart contract*. È stato pertanto evidenziato che, sebbene siffatta caratteristica sia in grado di offrire molti benefici (si pensi al citato esempio dei rimborsi dei biglietti aerei), consente tuttavia di attribuire "*buona fede a due parti naturalmente in mala fede*"[10]. Detto più chiaramente: l'automatismo e l'irreversibilità che contraddistinguono il funzionamento degli *smart contract* riducono il comune (e significativo) rischio che le parti dell'accordo criminale recedano, si ritirino, o tradiscano la controparte nel corso dell'esecuzione del reato, rendendo così sicure tutte le transazioni di carattere illecito e attribuendo (appunto) "*buona fede a due parti* [criminali, che si trovano] *naturalmente in mala fede*".

Un terzo (e non meno rilevante) aspetto "problematico" degli *smart contract* discende poi dalla minimizzazione del rapporto tra le parti durante l'esecuzione dell'accordo. La descritta natura "automatica" dello *smart contract* fa infatti sì che per monitorare l'esecuzione (ad esempio) di una prestazione illecita, non sia più necessario alcun contatto od incontro tra mandante ed esecutore, giacché siffatta verifica verrà svolta in maniera autonoma dallo stesso *smart contract*. La dottrina ha perciò sottolineato come una siffatta situazione renda pressoché impossibile identificare "*i mandanti dei reati che, dopo aver ideato il reato ed averlo trasformato in un codice per smart contract, possono restare completamente anonimi e slegarsi dal contratto stesso*"[11].

Il quarto profilo di indagine risiede nuovamente nel fatto che gli *smart contract* consentono (e consentiranno ancor più in futuro) di utilizzare anche fonti esterne, di carattere aperto, come *input* di verifica dell'avvenuta esecuzione dell'accordo, quali ad esempio bollettini meteo, listini ufficiali di prezzi di azioni, articoli di stampa etc. Si è invero già chiarito come anche siffatte funzionalità finiscano (e finiranno) non solo per ridurre ulteriormente l'esigenza di interazione tra mandante ed esecutore materiale del reato, ma per allargare il raggio di azione degli *smart contract* dal mondo virtuale a quello fisico e reale, potendo così agevolare e rendere più sicura la commissione di gravi reati su commissione quali (ad esempio) omicidi, crimini di terrorismo, lesioni, incendi dolosi etc. (vedi *infra*)[12].

---

[9] L. SHLOMI, N. STAKHANOVA, and A. MATYUKHINA, *Exploring Ethereum's blockchain anonymity using smart contract code attribution* in *15th International Conference on Network and Service Management (CNSM)*, IEEE, 2019. Le autrici hanno chiarito come sia possibile ricondurre lo *smart contract* alle chiavi pubbliche dei relativi autori. Ad ogni modo, non è possibile risolvere il problema della riconducibilità della chiave pubblica visibile sulla *blockchain* al soggetto fisico effettivo titolare.

[10] A. JUELS, A. KOSBA, E. SHI, *The ring of gyges: Using smart contracts for crime*, cit., p. 54

[11] *Ult. Op. cit.*

[12] *Ult. Op. cit.*

3. I c.d. "*criminal smart contract*".

La dottrina per ora formatasi[13] ha individuato due tipologie di *smart contract* che potrebbero essere "sfruttate" dalla criminalità. I c.d. *criminal smart contract* ed i *vulnerable smart contract*. Mentre i primi vengono definiti come "*smart contract che facilitano la commissione di reati tramite criptovalute nei sistemi distribuiti*"[14], con il termine *vulnerable smart contract* la dottrina indica invece quei contratti che, contenendo errori ("*bugs*") nel proprio codice di esecuzione, possono venire utilmente "attaccati" da terzi aggressori con l'intento di modificarne il contenuto e/o di rubare l'oggetto della transazione (*recte*: della quantità di criptovaluta idonea al saldo dell'operazione dedotta in contratto). Si tratterà qui dunque della sola prima categoria di *smart contract* (i c.d. *criminal smart contracts*), poiché le due tipologie di contratti presentano caratteristiche criminogene molto diverse e (soprattutto) il concetto di *bug* insito nei *vulnerable smart contract* imporrebbe disamine distinte e specifiche per ciascun singolo contratto[15].

Bene allora chiarire che la dottrina si è ad oggi focalizzata su due tipiche e distinte categorie di *crininal smart contract*:

- i *criminal smart contract* strutturati per ottenere la rivelazione di informazioni segrete o di chiavi private (ad es. le chiavi di accesso ad un *wallet* contenente valuta virtuale);

- e i *criminal smart contract* cosiddetti "*calling card crimes*" ("crimini con biglietto da visita") che si caratterizzano per la circostanza che la loro esecuzione abbia effetto nella realtà fisica e non in quella propriamente digitale[16].

Muovendo dalla prima categoria, tra i principali *criminal smart contract* finalizzati al furto di informazioni sono stati (intanto) individuati quelli adibiti alla rivelazione di informazioni sottoposte a segreto. In specifico, lo *smart contract* viene in questo caso programmato in modo tale che, una volta corrisposto il prezzo in criptovaluta, il contratto stesso renda automaticamente decriptata (e quindi visibile) l'informazione riservata dedotta in contratto per un determinato periodo di tempo. Si tratta cioè di accordi che sono idonei a dar vita a dei veri e propri mercati di informazioni riservate riguardanti (ad esempio) segreti governativi o industriali[17].

Una seconda tipologia di *criminal smart contract* rientrante nella medesima categoria prevede poi che, all'effettuazione di un modesto pagamento, venga decriptata solo una parte delle informazioni riservate. Laddove le stesse risultino "interessanti" per

---

[13] Per ora gli studi sono relativi all'ideazione e al funzionamento di tali contratti *smart* da un punto di vista tecnico.

[14] M. NDIAYE, P.K. KONATE, *Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain*, cit.

[15] Per una definizione e trattazione (dal punto di vista tecnico) dei *vulnerable smart contract* si rimanda a: M. NDIAYE, P.K. KONATE, *Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain*, cit.

[16] M. NDIAYE, P.K. KONATE, *Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain*, cit.; A. JUELS, A. KOSBA, E. SHI, *The ring of gyges: Using smart contracts for crime*, cit., p. 54.

[17] *Ult. Op. cit.*

l'utente, una volta corrisposto il saldo, il contratto decripterà la restante parte delle informazioni. Di contro, laddove quanto esibito non susciti interesse, le informazioni saranno nuovamente criptate ed al contraente verrà rimborsato il contributo iniziale. Questo tipo di *criminal smart contract* permette pertanto l'efficace rivelazione di informazioni riservate, consentendo ai detentori di monetizzarne l'integrale *disclosure* nella più completa anonimità e semplicità[18].

Ulteriore esempio di *criminal smart contract* della tipologia in esame è quella dei c.d. "*key compromise criminal smart contract*": una tipologia di contratti finalizzata al furto di chiavi informatiche e che prevede il trasferimento automatico di criptovaluta al soggetto che comunichi allo *smart contract* la chiave privata corretta[19]. Si tratta (in buona sostanza) di un contratto che sollecita e commissiona il furto di chiavi private di acceso. In specifico, una volta concluso l'accordo, il criminale informatico tenterà di decriptare la chiave privata di accesso e, una volta individuata, la comunicherà allo *smart contract*. Quest'ultimo provvederà poi automaticamente a verificare se la chiave comunicata consenta effettivamente l'accesso al sistema protetto e (in caso positivo) a corrispondere il compenso in criptovaluta al pirata informatico.

La seconda (ed ancor più allarmante) categoria di *criminal smart contract* è senz'altro costituita dai c.d. *calling card crimes* (o crimini dal biglietto da visita). Come già anticipato, i sistemi atti ad incorporare gli *smart contract* – come ad esempio la *blockchain* di Ethereum – consentono (e consentiranno ancor più in futuro) la verifica di avveramento delle condizioni contrattuali in ragione di fattori esterni (ad es: bollettini meteo, listini ufficiali di prezzi di azioni, articoli di stampa). I *calling card crimes* sono appunto i *criminal smart contract* che utilizzano siffatta tecnologia e che possono perciò agevolare la commissione di gravi reati che si manifestano nel mondo fisico quali (ad esempio) gli omicidi su commissione.

L'esempio tipico è rappresentato in dottrina come "*Caso del Senator X*". Lo *smart contract* "*Contratto*" prende come *input* da un esecutore del contratto "*P*" un impegno "*vcc*" che specifica in anticipo i dettagli (giorno, ora e luogo) dell'assassinio del senatore. Per reclamare la ricompensa, l'esecutore P disattiva ("*decommit*") l'impegno "*vcc*" dopo aver effettuato l'assassinio e per verificare quanto affermato da P, il "*Contratto*" cerca in automatico un *feed* di dati pubblici autenticati sulle notizie che confermino l'assassinio del Senatore X con i dettagli corrispondenti all'impegno "*vcc*" stabilito in contratto (ad es. articoli di stampa che confermino l'avvenuto assassinio, necrologi). Una volta verificato che l'assassinio del Senatore X sia effettivamente avvenuto con i dettagli corrispondenti all'impegno "*vcc*", il contratto pagherà quindi in automatico all'esecutore "*P*" la ricompensa pattuita in criptovaluta[20].

Manifesto come i *calling card crimes*, a cui si affianca il graduale maggiore sviluppo di *smart contract* alimentabili tramite *feeds* provenienti dal mondo esterno, possano così costituire una struttura generalizzata per il compimento di un'assai ampia varietà di gravi reati su commissione. Per vero, nelle possibili applicazioni di questo tipo

---

[18] *Ult Op. cit.*

[19] *Ult. Op. cit.*

[20] A. JUELS, A. KOSBA, E. SHI, *The ring of gyges: Using smart contracts for crime*, cit., p. 54.

di *criminal smart contract* rientrano (con agio) i rapimenti, i sabotaggi, gli attacchi informatici o terroristici, reati di lesioni, incendi, epidemia: praticamente tutto quanto possa essere verificato e contenuto in un *data feed* esterno (ad esempio notizie di stampa) può (e potrà) essere designato come obiettivo di un *calling card crimes*.

Il chiaro allarme sociale suscitato da siffatte considerazioni risulta poi accresciuto a considerarsi altresì che, dopo aver perfezionato il contratto, nessuna interazione sarà necessaria tra il mandante e l'esecutore materiale dell'illecito, poiché sarà (appunto) lo *smart contract* a verificare, sulla base dei *feed* esterni, l'effettiva esecuzione dell'illecito ed a corrispondere il compenso pattuito.

Si osservi peraltro che la tecnologia sottesa al funzionamento di siffatti contratti è ancora in fase embrionale. La realizzazione di un sistema "*calling cards crimes*" realmente funzionale, versatile e adattabile alle varie transazioni che possano essere effettuate dipende infatti da una serie di problematiche tecniche che non constano essere state ancora pienamente risolte. Quanto resta da perfezionare è in specifico la c.d. tecnologia degli "oracoli", ossia un sistema capace di decriptare con precisione i *feeds* esterni che confermino l'avvenuta corretta esecuzione dell'azione criminale da parte del suo autore materiale e dunque corrispondergli, in modo automatico, l'importo dedotto nello *smart contract*[21].

È intuitivo dunque che le descritte potenzialità criminogene suggeriscano da subito la necessità dello sviluppo di una riflessione intesa a comprendere quali rimedi siano ipotizzabili in chiave preventiva e repressiva del fenomeno e, segnatamente, se e quale ruolo possa essere oggi giocato dal diritto penale "tradizionale" nella gestione di siffatti fenomeni tecnologici.

4. Il sistema *blockchain* nella concreta (in)operatività del diritto penale.

Qualunque possibile valutazione in merito al ruolo che possa giocare il diritto penale nel reprimere condotte illecite attuabili tramite *smart contract* non può prescindere dal dato dall'anonimato (*recte*: pseudoanonimato) che contraddistingue siffatto genere di transazioni. Come si è rappresentato, le parti di uno *smart contract* non sono nominativamente identificabili, poiché quanto solo visibile sulla *blockchain* sono le relative chiavi pubbliche di accesso al sistema. Il che comporta un'evidente difficoltà nell'individuare gli autori delle condotte illecite che vengano realizzate tramite *smart contract*. È invero di immediata evidenza che, nel caso in cui il commesso reato non riverberi i propri effetti nel mondo fisico (come ad esempio potrebbe verificarsi nel caso dei c.d. *calling card crimes*) sarà estremamente complicato (*recte*: pressoché impossibile) individuare non solo il mandante, ma anche l'esecutore materiale della condotta illecita; tanto più a considerarsi che la tecnologia in parola minimizza la necessità di comunicazioni ed interazioni tra le parti nel corso dell'esecuzione dell'accordo criminoso.

---

[21] L. BRUNONI, O. BEAUDET-LABRECQUE, *Smart contracts and cybercrime: a game changer?*, cit., p. 136-140.

In ottica preventiva (e repressiva) questo porta a domandarsi se sia (o meno) possibile individuare responsabilità penali in capo a soggetti che non partecipino direttamente alla commissione del fatto tipico di reato attuato mediante l'utilizzo di *criminal smart contract*, ma che ne agevolino comunque la commissione (i) o perché gestiscono la *blockchain* su cui viene distribuito ed eseguito il contratto con oggetto illecito (ii) o perché abbiano materialmente sviluppato il *software* (i.e. lo *smart contract*) concretamente utilizzato per commettere il reato.

In assenza di alcuna previsione legislativa è intanto possibile domandarsi se sul soggetto gestore della *blockchain* sussista (o meno) una facoltà (possibilità) di controllo dei contenuti diffusi nel sistema distribuito e se la sua posizione (e conseguente modello di responsabilità) possa essere quindi in qualche modo assimilabile a quella dell'*Internet Service Provider* (di seguito anche solo ISP).

In astratto potrebbe anzi sostenersi un "parallelismo" tra la posizione dei gestori delle infrastrutture decentralizzate e quella degli ISP, in quanto entrambe le attività consistono nel mettere a disposizione di un certo numero di utenti servizi consistenti nella registrazione e nella trasmissione di dati informatici. Medesime parrebbero perciò le esigenze connesse all'individuazione di un destinatario dei doveri di collaborazione con l'Autorità per impedire la commissione di reati o attenuarne le conseguenze lesive, soprattutto nel caso in cui siano rinvenibili all'interno del sistema *blockchain* (così come avviene per gli ISP) soggetti in posizione apicale o con possibilità di esercitare un qualche controllo sulla piattaforma.

Bene allora chiarire subito che le *blockchain* non sono tutte di identica natura, ma si possono distinguere in *unpermissioned blockchain* (o *blockchain* pubbliche) e *permissioned blockchain* (o *blockchain* private). In specifico, la *unpermissioned blockchain* (o "pubbliche") sono sistemi aperti e privi di alcuna entità gerarchicamente sovraordinata. La loro struttura è completamente decentralizzata e non hanno alcuna restrizione di accesso. Nessun utente ha dei privilegi sugli altri e nessuno può controllare le informazioni che vengano memorizzate su di essa, modificarle od eliminarle.

Siffatte caratteristiche fanno perciò si che non sia neppure astrattamente possibile pensare di replicare il modello di responsabilità previsto per gli ISP quando si abbia riguardo alle *unpermissioned blockchain*. Come pure noto, la possibile responsabilità degli ISP è infatti incentrata sulla presenza di un soggetto giuridico in posizione apicale rispetto agli altri, verso cui siano quindi esigibili determinati comportamenti volti a prevenire la diffusione e/o comunque eliminare eventuali contenuti illeciti che siano stati caricati sulla piattaforma.

Parzialmente diversa parrebbe invece essere l'ipotesi con riguardo alle *permissioned blockchain*. Siffatta tipologia di *blockchain* non è invero accessibile indiscriminatamente a tutti, ma prevede che uno o più soggetti definiscano i criteri di accesso e quali ruoli ciascun utente possa ricoprire all'interno della rete. Di più, in questa tipologia di struttura i dati, al momento dell'inserimento, sono sottoposti alla verifica di un gruppo ristretto di autori preventivamente autorizzati che mantiene pertanto una signoria sul funzionamento della rete.

Siffatte caratteristiche rendono perciò astrattamente ipotizzabile che alle *permissioned blockchain* possa venire applicata la disciplina dettata per gli ISP dalla

Direttiva n. 2000/31/CE ("Direttiva sul commercio elettronico"), poi recepita in Italia con il D.Lgs. 9 aprile 2003 n. 70. In specifico la predetta normativa pone (come noto) un generale limite alla Responsabilità degli ISP per gli illeciti commessi dai propri utenti (c.d. scudo di responsabilità o *safe harbour*[22]) che trova un solo limite nel fatto che l'ISP venga comunque a conoscenza della natura illecita del contenuto "caricato" sulla propria piattaforma e non si attivi prontamente per la relativa rimozione.

La dottrina e la giurisprudenza assolutamente maggioritarie (con un'unica sola eccezione[23]) sono giunte alla comune conclusione che la responsabilità dell'ISP per omessa rimozione di un contenuto di carattere illecito abbia rilievo soltanto civile, non potendosi invece configurare, in capo all'ISP, alcun profilo di responsabilità di carattere penale. L'articolo 17 del D.Lgs. 9 aprile 2003 prevede invero testualmente che l'ISP "*non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite*", sicché difetta qualunque posizione di garanzia sulla quale ancorare un'eventuale ipotesi di responsabilità penale *ex* art. 40 cpv c.p[24]. Il che vale (a *fortiori*) anche rispetto al gestore di una *permissioned blockchain*, per il quale manca addirittura qualsivoglia normativa di riferimento che consenta anche solo di ipotizzare la possibilità di sussistenza di una posizione di garanzia e dunque di configurare, a suo carico, una responsabilità penale di carattere omissivo improprio.

Al di là dell'aspetto strettamente giuridico mette poi (in ogni caso) conto considerare che la *blockchain* è un sistema che si fonda sull'immutabilità ed inalterabilità dei blocchi che la compongono. Anche laddove il legislatore intendesse effettivamente

---

[22] L. PICOTTI, *Obblighi di tutela penale degli Internet Service Providers* e *sviluppi della giurisprudenza europea* in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale-Cybercrime,* Milano, 2019, p. 81-96.

[23] Cfr. sul punto Cass. pen., sez. V, 27 dicembre 2016, n. 54946, in *Foro.it*.

[24] La dottrina in merito è ampia, *ex multis*: G. P. ACCINNI, *Profili di responsabilità penale dell'hosting provider "attivo"*, in *Arch. pen.*, fasc. 2, maggio-agosto, 2017; A. BACCIN, *Responsabilità penale dell'internet service provider e concorso degli algoritmi negli illeciti online: il caso Force v. Facebook*, in *Sist. pen.*, 1/2020, p. 5 ss.; R. BARTOLI, *Brevi considerazioni sulla responsabilità penale dell'Internet Service Provider,* in *Dir. pen. proc*., 2013, p. 600.; G. CORRIAS LUCENTE, *Ma i network providers, i service providers e gli access providers rispondono degli illeciti penali commessi da un altro soggetto mediante l'uso degli spazi che lo gestiscono*? in *Giur. mer.*, 2004, p. 2523 ss.; G. FORNASARI, *Il ruolo dell'esigibilità nella definizione della responsabilità penale del provider*, cit., p. 423 ss.; A. INGRASSIA, *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?* in *Dir. pen. cont*., 8 novembre 2012; A. INGRASSIA, *La sentenza della Cassazione sul caso Google*, in *Dir. pen. cont.*, 6 febbraio 2014 (nota a sentenza); A. INGRASSIA, *Responsabilità penale degli internet service provider: attualità e prospettive*, in *Dir. pen. proc*., 2017, 12, p. 1261 ss.; R. E. MAURI, *Applicabile l'art. 57 c.p. al direttore del quotidiano online: un revirement giurisprudenziale della cassazione, di problematica compatibilità con il divieto di analogia*, in *Dir. Pen. cont.*, 28 febbraio 2019 (nota a sentenza); PANATTONI B., *Il sistema di controllo* successivo…, cit.; D. PETRINI, *Il direttore della testata telematica, tra* horror vacui *e prospettive di riforma; sperando che nulla cambi*, in *Riv. it. dir. proc. pen.*, 2012,4, p. 1611 ss.; R. PETRUSO, *Responsabilità degli intermediari di internet e nuovi obblighi di conformazione: robo-takedown, policy of termination, notice and take steps*, In *Eur. dir. priv.*, 2017, 2, P. 451 SS.; L. PICOTTI, *La responsabilità penale dei service providers in Italia*, In *Dir. pen. proc.*, 1999.; L. PICOTTI, *fondamenti e limiti della responsabilità penale dei Service Providers in Internet,* in *Pen. Proc.*,1999; L. PICOTTI, *Obblighi di tutela penale degli Internet Service Providers* e *sviluppi della giurisprudenza europea*, cit.; S. SEMINARA, *La responsabilità penale degli operatori su internet*, in *Dir. inform*., 1998, 4-5, p. 745 ss; S. TURCHETTI, *L'art. 57 c.p. non è applicabile al direttore del periodico online*, in *Dir. Pen. cont.*, 17 novembre 2010 (nota a sentenza); V. NARDI, *I discorsi d'odio nell'era digitale: quale ruolo per l'*Internet Service Provider?, in *Dir.pen.cont*., 7 marzo 2019.

introdurre un obbligo giuridico di eliminare dalla *blockchain* (ad esempio) lo *smart contract* dal contenuto illecito, siffatto obbligo sarebbe pertanto inattuabile *ex se* ed inesigibile, poiché l'eliminazione del "blocco" contenente il *criminal smart contract* determinerebbe (semplicemente) l'invalidazione stessa dell'intera struttura.

5. L'astratta (ir)responsabilità concorsuale dello sviluppatore dello *smart contract*.

Esclusa dunque l'ipotetica responsabilità penale del gestore della *blockchain* (sia essa *permissioned* o *unpermissioned*) residua la possibilità di interrogarsi in merito ad una (pure ipotetica) responsabilità concorsuale dello sviluppatore del *criminal smart contract* rispetto al reato fine che gli autori materiali abbiano commesso per il tramite del suo utilizzo.

In specifico, l'operatività per il tramite di *smart contract* può avvenire secondo due modalità distinte tra di loro. Le parti possono concludere da sé uno specifico accordo in linguaggio computazionale (*smart contract* proprio), oppure possono concordare sul contenuto di uno *smart contract* già sviluppato e registrato in *blochchain* ad opera di un terzo (c.d. *smart contract* improprio o di terza parte). Sarebbe allora ipotizzabile un concorso del terzo sviluppatore del *criminal smart contract* rispetto al reato commesso da due parti diverse (mandante ed esecutore materiale) tramite il suo utilizzo?

Per rispondere al quesito si può affermare che, mentre sorgono minori problemi relativamente alla configurazione del contributo causale fornito dall'autore dello *smart contract* alla commissione del fatto tipico, ben maggiori perplessità suscita la possibile attribuzione, in capo a quest'ultimo, del dolo tipico del concorso di persone nel reato[25]. Noto infatti che, per potersi configurare una responsabilità concorsuale, si richiede (da un lato) che il concorrente fornisca un contributo causale alla commissione del fatto di reato, dall'altro che questi agisca (appunto) con dolo: la particolare struttura del fatto nel concorso di persone comporta che l'oggetto del dolo abbracci sia il fatto principale realizzato dall'autore materiale, sia il contributo causale recato dalla condotta atipica alla commissione di quel fatto[26].

La tematica del concorso si interseca così con quella della natura *dual use* dei *software* che contraddistingue quei programmi che possono essere utilizzati sia per scopi leciti che illeciti. Detto più chiaramente: laddove lo *smart contract* venga progettato secondo uno schema di per sé neutro (ad es. io configuro uno *smart contract* affinché, al verificarsi di determinate condizioni non preimpostate, venga eseguito un pagamento), risulterà difficile (*recte*: impossibile) provare la consapevolezza e la volontà dello sviluppatore non solo rispetto al fatto principale, ma anche al contributo causale recato dalla condotta atipica (sviluppo di un *software dual use*) alla commissione dello specifico

[25] Le parti possono concordare sul contenuto di un contratto già registrato in *blockchain* ad opera di un terzo (*smart contract* improprio o di terza parte), ovvero concludere da sé un accordo in linguaggio computazionale (*smart contract* proprio).

[26] Per tutti, G. MARINUCCI-E. DOLCINI, *Manuale di diritto penale: parte generale*, Milano, 2017, pp. 493 ss.

fatto di reato. Ragionando diversamente si finirebbe per ammettere (ad esempio) la responsabilità concorsuale del venditore di un coltello rispetto all'assassinio operato per il tramite del suo utilizzo, ossia ciò che (evidentemente) non può essere.

Residua però il dubbio se, a condizioni più precise, il giudice possa pervenire a diverse conclusioni. In specifico, nei limiti in cui il *criminal smart contract* non nasca come prodotto *dual use*, ma finalizzato esclusivamente alla commissione di uno specifico e determinato reato, si potrebbe astrattamente argomentare che lo sviluppatore si sia rappresentato ed abbia voluto la commissione di quello stesso crimine e sia così possibile il riconoscimento di un dolo concorsuale rispetto a siffatto reato fine.

Si pensi al caso di uno sviluppatore che configuri un *criminal smart contract* della tipologia *calling card crimes* secondo cui, comprovato l'evento morte per assassinio del "Senatore X" mediante *feed* esterni prestabiliti (ad es. notizie di stampa), il contratto paghi autonomamente la ricompensa all'esecutore "P" che abbia disattivato l'impegno "vcc" dopo aver commesso l'assassinio. In questo caso parrebbe astrattamente argomentabile il dolo tipico del concorso di persone in capo allo stesso sviluppatore del contratto, che potrebbe perciò essere chiamato a rispondere di concorso in omicidio in uno con il mandante (che abbia pagato il corrispettivo per il delitto) e con il suo esecutore (che abbia commesso materialmente l'omicidio ed abbia ricevuto il pagamento).

Nondimeno, al di là dei casi limite, occorre considerare che gli *smart contract* si connotano (per loro natura) per nascere pressoché sempre come prodotti *dual use* e come resti pertanto estremamente complicato determinarne la finalizzazione univoca alla commissione di uno specifico reato piuttosto che a regolare leciti rapporti giuridici tra le parti. Chiaro insomma come anche la "strada" del concorso dello sviluppatore del *software* nel reato preso di mira dai relativi utilizzatori (anche nel caso di *criminal smart contract*) si palesi senz'altro complicata ed assai difficile da essere percorsa.

6. Profili di applicabilità degli artt. 615-*quater* c.p. e 615-*quinquies* c.p.

Resta allora che nel quadro normativo attualmente vigente vi sono alcune disposizioni che, in un'ottica anticipatoria della tutela penale, puniscono azioni consistenti nel procurarsi o diffondere programmi intrinsecamente pericolosi. Tra queste si possono menzionare le fattispecie incriminatrici di cui agli artt. 615-*quater* c.p. e 615-*quinquies* c.p[27].

[27] In argomento v. A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale-Cybercrime,* cit., p. 692 ss. Si segnala che le norme sono state oggetto di una recente modifica legislativa (avvenuta tramite l'art. 19, comma 1, lett. c), l. 23 dicembre 2021, n. 238) che ha inciso sulla rubrica sulle condotte e sulla cornice edittale dell'art. 615 *quater* c.p. Le modifiche sono entrate in vigore dal 1° febbraio 2022 ed è rilevante sottolineare il consistente ampliamento delle condotte sanzionate sia dal testo della disposizione di cui all'art. 615 *quater* c.p., sia da quello di cui all'art. 615 *quinquies* c.p. Per un commento si veda Corte Suprema di Cassazione (Ufficio del Massimario), *Relazione su novità normativa: la legge 23 dicembre 2021 n.238, disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2019-2020*, 21 marzo 2022, p. 6-

L'art. 615-*quater* c.p. punisce in specifico chi "*al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti*[28]*, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni*[29] *e con la multa sino a 5.164 euro.*".

Oggetto di sanzione sono cioè le condotte di chi "*mette in altro modo a disposizione*" di terzi ("*si procura*" "*diffonde*" "*comunica*" ovvero "*consegna*") *software*[30] idonei a consentire l'accesso ad un sistema informatico protetto da misure di sicurezza[31].

La dottrina ha dunque chiarito che la natura "aperta" della disposizione (ben rappresentata dalla locuzione "*altri mezzi idonei all'accesso*") permetta di ricondurre nell'alveo dell'art. 615-*quater* c.p. tutti i comportamenti che consistano nel procurarsi o nel mettere a disposizione "*le tecniche atte ad introdursi abusivamente in un sistema informatico altrui*"[32]. In altri termini, la fattispecie ha ad oggetto condotte "*prodromiche e preparatorie alla commissione di un reato informatico (ad es. accesso abusivo ad un sistema informatico o frode informatica)*" che "*si colorano in termini di intrinseca pericolosità per il bene giuridico […] qualora abbiano ad oggetto un programma informatico che può essere oggettivamente impiegato per commettere un fatto penalmente rilevante*"[33]. In altri termini, non esiste una definizione che individui *a priori* quali programmi informatici debbano ritenersi intrinsecamente illeciti. Si dovrà invece fare riferimento ai fini perseguiti dall'utente o dal programmatore, ovvero all'attitudine del programma ad agevolare la commissione di accessi illeciti all'altrui sistema informatico.

Stanti tali caratteristiche parrebbe potersi trattare di una fattispecie funzionale al perseguimento degli sviluppatori (almeno) di alcune determinate tipologie di *criminal smart contract*. Si pensi, ad esempio, ai richiamati *criminal smart contract* strutturati per ottenere la rivelazione di informazioni segrete o di chiavi private e, in specifico, a quelli programmati in modo tale che, una volta corrisposto il prezzo in criptovaluta, il contratto stesso renda automaticamente decriptata (e quindi visibile) l'informazione riservata dedotta in contratto per un determinato periodo di tempo. Analogo riferimento può essere poi operato a quei *criminal smart contract* per cui, all'effettuazione di un

---

9; C. CRESCIOLI, C. GRECO, B. PANATTONI, M. PITTIRUTI, R. M. VADALÀ, *Cybercrime: rassegna delle novità (Gennaio-Febbraio 2022)*, in *Sist. Pen.*, 13 maggio 2022.

[28] I termini "*si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti*," sono stati sostituiti alle parole "*si procura, riproduce, diffonde, comunica o consegna*" dall'art. 19, comma 1, lett. a), l. 23 dicembre 2021, n. 238.

[29] Le parole "*sino a due anni*" sono state sostituite a quelle "*sino ad un anno*" dall'art. 19, comma 1, lett. a), l. n. 238, cit.

[30] La norma fa generico riferimento ad "*apparati, strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico*".

[31] A. CAPPELLINI, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Trattato di diritto penale – Cybercrime*, cit., p. 692 ss. p. 693.

[32] *Ult. Op. cit.*, p. 694.

[33] *Ult. Op. cit.*, p. 695.

modesto pagamento, venga decriptata solo una parte delle informazioni riservate e, laddove queste risultino "rilevanti", segua il decriptaggio delle informazioni mancanti.

Maggiori problematicità comporta invece la possibilità di inquadramento all'interno della stessa descritta fattispecie di altri tipi di *criminal smart contract*, quali, ad esempio, il "*key compromise criminal smart contract*". In questo caso lo *smart contract* viene infatti utilizzato esclusivamente per consentire un pagamento anonimo al soggetto che materialmente si occupi di reperire in modo abusivo la chiave privata, ma non viene direttamente utilizzato per accedere a contenitori di dati informatici protetti da misure di sicurezza. Medesimo ragionamento potrebbe peraltro essere fatto (*a fortiori*) per i c.d. "*calling card crimes*", in quanto siffatti *criminal smart contract* possono venire utilizzati per commettere reati aventi effetto sul mondo esterno, fisico, e non per accedere abusivamente a sistemi informatici altrui.

Ciò posto, passando all'esame della fattispecie di cui all'art. 615-*quinquies* c.p.[34], vi è che la disposizione punisce "*chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene*[35]*, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa*[36] *apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.*".

Anche in questo caso, si puniscono quindi condotte "preparatorie" alla commissione dei reati di danneggiamento e/o (comunque) all'alterazione di sistemi ovvero di informazioni informatiche. Non è richiesto neppure che i programmi oggetto materiale della norma siano principalmente adattati o ideati per commettere il reato informatico, tanto che si è osservato come "*anche chi consegna un programma informatico di per sé lecito […] verrebbe ad essere punito qualora agisse al fine di commettere un danneggiamento di dati o di sistemi informatici […]*"[37].

Sebbene sia stato evidenziato come, per tale via, il Legislatore abbia tipizzato una condotta priva di offensività oggettiva[38], resta che l'ampiezza della fattispecie la renda a propria volta fungibile a reprimere la diffusione di *criminal smart contract*. Chiaro infatti che gli *smart contract* destinati a decriptare abusivamente informazioni riservate possano sicuramente venire ricompresi in quelli finalizzati all'alterazione di sistemi informatici o (comunque) all'alterazione/danneggiamento del funzionamento del database contenente le informazioni che si intendano trafugare.

---

[34] Articolo (anch'esso) modificato nella rubrica e nella condotta incriminata dall'art. 19, comma 2, l. 23 dicembre 2021, n. 238. Le modifiche sono entrate in vigore dal 1° febbraio 2022. Relativamente alle modifiche che hanno in via principale ampliato le condotte punibili, si rinvia alla nota 27.

[35] Le parole "*abusivamente si procura, detiene*," sono state sostituite alle parole "*si procura*" dall'art. 19, comma 2, lett. a), l. n. 238, cit.

[36] Le parole "*abusivamente si procura, detiene*," sono state sostituite a quelle "*mette a disposizione di altri*" dall'art. 19, comma 2, lett. a), l. n. 238, cit.

[37] *Ult. Op. cit.*, p.703.

[38] I. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "*dual-use software", in *Rivista italiana di diritto e procedura penale*, 2017, p.764.

In conclusione, entrambe le fattispecie incriminatrici esaminate parrebbero astrattamente applicabili allo sviluppatore di *criminal smart contract*. Per vero, poiché le stesse puniscono anche la mera signoria sul *software* criminale (è punito chi produce, ma anche chi "*si procura*" il software), potrebbe ricadere nel fuoco della norma anche un soggetto terzo distinto dallo sviluppatore quale (appunto) colui che si procuri il *software* comprendente il *criminal smart contract* per poi utilizzarlo sulla *blockchain*.

Vero, tuttavia, che l'applicazione pratica di tali fattispecie resta (in ogni caso) problematica, in quanto è raro che un *software* venga concepito esclusivamente per commettere un reato o che si accerti l'effettiva finalità dello sviluppatore. Come pure si è rappresentato, spesso ci si trova infatti davanti a *software* multifunzione (o *dual use*) utilizzabili indistintamente per fini leciti ed illeciti; con la conseguenza che per giungersi ad una corretta incriminazione occorrerebbe preliminarmente stabilire se la funzione del *software* in rilevo sia prevalentemente lecita od illecita: ciò che risulta evidentemente foriero di gravi complicanze[39].

7. Conclusioni: il progresso tecnologico tra auto responsabilizzazione e minaccia di pena.

Conclusivamente si può rappresentare che la tecnologia *blockchain,* in continua espansione, accresce la difficoltà di stabilire regole "fisse" relativamente al suo funzionamento ed eventuali responsabilità. Il Legislatore, per i settori in via di sviluppo (*in primis* il settore internet e gli ISP), ha sino ad ora optato perciò per concedere agli operatori la possibilità di autodisciplinarsi, limitandosi a dettare solo principi a cui conformarsi per permettere così un rapido sviluppo di tecnologia nell'ottica di migliorare le condizioni di vita di tutti[40].

In ragione delle tematiche che si sono diffusamente riportate nelle pagine precedenti, pare nondimeno assai opportuno avviare una più compiuta riflessione sulle possibili implicazioni criminali della *blockchain*, senza cioè limitare lo spettro di indagine a quelle (già note) relative ai reati di riciclaggio. Come si è rappresentato, applicare le regole proprie del diritto penale tradizionale configurando (ad esempio) una responsabilità omissiva autonoma in capo al gestore del sistema *blockchain* (ideando posizioni di garanzia "generali"[41]), oppure configurando una responsabilità concorsuale dello sviluppatore del *criminal smart contract*, significherebbe giocare d'azzardo con il diritto penale.

---

[39] Vanno quindi individuati i connotati tipici che permettano di selezionare con sufficiente determinatezza e precisione i programmi informatici che si caratterizzano per la loro intrinseca pericolosità e perché possono assurgere ad oggetto materiale di un reato – I. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale,* cit., p. 753.

[40] M. GAMBINI, *Le responsabilità civili dell'Internet service provider*, Edizioni Scientifiche Italiane, 2006, p. 227–321.

[41] Possibilità che, inoltre, la dottrina esclude. G. MARINUCCI-E. DOLCINI, *Manuale di diritto penale*, cit., p. 248.

Allo stesso modo, le stesse disposizioni anticipatorie della tutela penale di cui agli artt. 615-*quater* e 615-*quinquies* c.p., nonostante la loro più ampia fungibilità, risultano in concreto difficilmente applicabili a scongiurare il fenomeno della diffusione di *criminal smart contract*, in ragione (appunto) della natura *dual use* di siffatti *software* e della difficoltà di individuarne la maggiore o minore "finalità criminosa" del singolo programma considerato.

Pare allora necessario prendere atto che, ad oggi, il diritto penale tradizionale ed i relativi schemi di imputazione non siano "attrezzati" a governare un fenomeno informatico in continua e rapida evoluzione. Per vero, il dibattito degli studiosi di *smart contract* si è solo di recente concentrato sulla possibilità di neutralizzare la proliferazione di *criminal smart contract* utilizzando la medesima tecnologia "*smart*", ossia attraverso lo studio di *software* in grado di individuare i contratti con finalità criminali[42]. Dal punto di vista dei presidi giuridici, parrebbe invece opportuno che il legislatore operasse nei confronti degli sviluppatori (e/o delle piattaforme di sviluppo) di *smart contract* nel senso di agevolare la responsabilizzazione del settore, introducendo cioè principi giuridici a cui conformarsi al fine di minimizzare il rischio di degenerazione criminogena della tecnologia *blockchain*[43]. E questo è certamente compito del diritto amministrativo attraverso gli strumenti del "comando" e del "controllo" che gli sono propri.

---

[42] Y. WANG et al, *Randomness invalidates criminal smart contracts*, in *Information Sciences* 477, 2019, p. 291-301; L. ZHANG et al., *A game-theoretic method based on Q-learning to invalidate criminal smart contracts*, in *Information Sciences* 498, 2019, p.144-153.

[43] Questo sembra essere l'approccio optato dal legislatore europeo in materia di responsabilità degli ISP: con il *Digital Service Act*, proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE. Il regolamento mira a introdurre regole più stringenti alle piattaforme richiedendo maggiori obblighi di trasparenza e controllo.