CAMERA DEI DEPUTATI N. **2342**

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

GRIMOLDI, BONIARDI

Modifica all'articolo 61 del codice penale, in materia di circostanze aggravanti per i reati commessi attraverso strumenti informatici o telematici, e introduzione dell'articolo 10-*bis* del codice di procedura penale, in materia di competenza per territorio relativamente ai medesimi reati

Presentata il 17 gennaio 2020

ONOREVOLI COLLEGHI ! – Definire informatici alcuni reati non deve essere un modo per classificare questi delitti, bensì un criterio per valutare la circostanza nella quale essi sono perpetrati, in quanto, nell'ambito di una condotta che lede uno specifico interesse, l'abuso del mezzo digitale, piuttosto che di un mezzo tradizionale, non comporta la commissione di un reato differente; si tratta invece di un fatto criminoso che emerge in un contesto diverso o in una diversa circostanza.

Classificare e raggruppare alcuni delitti sotto il titolo di reato informatico è una prassi errata in partenza; sarebbe, invece, corretto e coerente con i princìpi del diritto penale parlare di reati informatici quando il mezzo utilizzato per compiere il fatto è di tipo digitale, mentre si dovrebbe parlare di reati contro l'informatica – coerentemente con il linguaggio giuridico in uso – nel caso di delitti che recano danni ai sistemi informatici e al loro buon funzionamento, intesi come interesse della collettività meritevole di tutela in quanto replicazione ed estensione del domicilio nel campo digitale ovvero nel *cyber* spazio, un luogo virtuale all'interno del quale, oltre allo sviluppo della personalità dell'individuo, viene svolta e custodita una serie di attività proprie della scienza dell'informazione. I beni e gli interessi tutelati non rappresentano la discriminante tra reato e reato informatico, ma tra tipi di reato: il reato informatico non è, quindi, un tipo di reato, ma un delitto caratterizzato dall'uso

del mezzo digitale, qualsiasi sia l'oggetto dell'offesa.

Prendiamo in considerazione, a titolo esemplificativo, lo *stalking* ovvero l'atto persecutorio quale condotta delittuosa tipica del fenomeno del bullismo: tale reato rientra nei delitti contro la persona ed è normato dall'articolo 612-*bis* del codice penale. Lo *stalking* è stato rilevato per la prima volta negli anni sessanta nelle scuole scandinave; a quei tempi l'utilizzo dei *media* digitali non era contemplato e l'offesa si realizzava solo nel mondo materiale. Con l'avvento dell'era digitale l'atto persecutorio è diventato realizzabile anche per il tramite del mezzo informatico e ciò ha portato alla creazione del termine « *cyber*-bullismo ».

Questo è il primo segnale che ci deve far riflettere: è il cambio del mezzo che determina la caratteristica informatica del reato e non l'interesse leso.

A seguito della scelta del mezzo digitale come strumento per compiere il fatto osserviamo, innanzitutto, che l'interesse protetto dall'articolo 612-*bis* del codice penale si autolimita, per ragioni di fattibilità, alla sola sfera psichica a causa dell'assenza di contatto fisico tra i soggetti coinvolti e, quindi, dell'impossibilità di commettere violenza sulla persona.

Diversa è, quindi, la situazione ovvero la circostanza nella quale il soggetto decide di agire: lo *stalker* può agire di notte o di giorno, da solo o in gruppo e di persona o per interposizione del mezzo digitale. In qualsiasi caso, l'interesse leso è sempre lo stesso, il reato è il medesimo e quello che cambia è solo la circostanza.

Se il reato è lo stesso può essere utile utilizzare il termine di « *cyberstalking* » per inquadrare con un termine unico il reato e la circostanza, ma il delitto è sempre quello dell'atto persecutorio ovvero un reato contro la persona che, se consumato con un mezzo digitale, diventa reato informatico contro la persona. Il tipo di reato non cambia ed è pertanto assurdo replicare leggi attraverso nuove disposizioni ciascuna delle quali contempla una circostanza diversa: non si è mai fatto prima d'ora e non vi è motivo per cui debba essere fatto oggi quando abbiamo a disposizione circostanze aggravanti e attenuanti per graduare la gravità del delitto in funzione degli elementi accidentali che lo costituiscono.

A questo proposito si consideri, ad esempio, la frode informatica per la quale, ai sensi dall'articolo 640-*ter* del codice penale, il legislatore ha previsto una pena inferiore rispetto alla truffa, ma che nei fatti altro non è che una truffa informatica ovvero l'esercizio di un artifizio già contemplato dall'articolo 640 del medesimo codice e messo in essere con abilità tecnica al fine di procurarsi un ingiusto profitto: per tale motivo essa dovrebbe rientrare nella fattispecie di truffa aggravata in qualità di reato informatico contro il patrimonio e quindi con una pena decisamente superiore a quella attualmente prevista.

Allo stato attuale, tenuto conto degli spazi edittali, qualora il reato fosse possibile con modalità sia tradizionali sia informatiche, ci troveremmo nell'assurda situazione di dover ammettere che per il criminale che sta meditando su come agire l'opzione della frode informatica possa apparire come un reato meno grave e quindi da preferire rispetto alla truffa per conseguire, comunque, lo stesso risultato ma con mezzi diversi. Si osservi, inoltre, che qualora la frode informatica possa essere eventualmente configurata in giudizio anche come truffa, la prima – la frode informatica – prevarrebbe sulla seconda per via del principio di specialità del diritto penale. Dal punto di vista della sanzione penale risulta quanto meno ragionevole affermare che dovrebbe essere l'esatto contrario.

A conferma di quanto rilevato si consideri che è proprio la circostanza a cambiare e non il delitto nella sua essenza. Per quanto concerne il bullismo si valuta, infatti, l'eventuale uso di un'eccessiva violenza o la presenza del « branco » come elemento intimidatorio, mentre per quanto concerne il bullismo informatico – il *cyber*bullismo – sarebbe opportuno valutare il grado di abilità utilizzato, la difficoltà tecnica da superare per mettere in atto l'evento, il grado di pressione nell'uso del canale di comunicazione e la potenzialità di danno producibile dal *media* scelto per

agire. Questi sono tutti elementi accessori che aggravano o attenuano la gravità del reato all'interno della struttura del medesimo delitto, ma in una situazione diversa.

L'identificazione del luogo di consumazione del reato è di assoluta importanza sia per la ricostruzione dei fatti in fase di indagine sia per questioni di competenza territoriale e di assegnazione del giudice naturale.

Nel caso di un reato informatico la questione si fa più complessa rispetto ai delitti non digitali. Come già accennato, è in primo luogo più complessa la ricerca della verità, ma una volta ricostruiti i fatti nasce una questione di merito sull'individuazione del luogo di consumazione, tema rispetto al quale dottrina e giurisprudenza stanno ancora delineando i propri confini.

Il reato si definisce « consumato » quando tutte le condizioni che rendono criminosa una fattispecie sono soddisfatte e il luogo di consumazione è quello nel quale è soddisfatta l'ultima condizione necessaria a rendere un fatto specifico assimilabile alla fattispecie delittuosa normata.

Invero il reato esiste nel momento in cui l'ultimo tassello necessario alla costituzione della struttura delittuosa viene aggiunto e quindi, considerato che in assenza di un elemento di condotta il reato non sussiste, il reato è consumato nel luogo in cui è, appunto, posta in essere l'ultima azione necessaria.

La giurisprudenza ha dato diverse interpretazioni in materia di reati informatici: dal luogo in cui si trova il soggetto attivo fino al luogo di ubicazione del *server* oggetto del reato, con drammatici risvolti pratici in termini di competenza, quasi sempre a sfavore della vittima.

A giudizio dei proponenti la *ratio* di questi approcci dovrebbe essere drasticamente rivista.

Il concetto principale è che l'azione informatica si consuma in un mondo virtuale che, in quanto tale, sottende a regole fisiche diverse rispetto al mondo reale. Tempo e spazio, azione, luogo e mezzi seguono regole diverse nei due mondi e se si accetta come assioma fondamentale il principio che afferma l'esistenza di un domicilio virtuale come estensione di quello tradizionale si deve accettare che anche lo spazio d'azione virtuale è un'estensione di quello reale.

Un altro passaggio necessario è chiarire il concetto di estensione, ovvero dare forma al rapporto di relazione tra uno spazio e l'altro attraverso il quale trasliamo regole e norme affinché quelle previste per il mondo tradizionale valgano anche per quello virtuale. Le azioni e i fatti che possono essere compiuti nel mondo virtuale non possono sempre essere messi in atto in quello tradizionale. Si pensi, ad esempio, alla posta elettronica. Una lettera impiega giorni ad attraversare l'oceano; una *e-mail*, invece, raggiunge la propria destinazione in pochi millisecondi viaggiando alla velocità dell'elettrone e, in alcuni tratti di fibra, anche alla velocità della luce, per poi magicamente comparire dall'altra parte del mondo sotto forma di copia dell'originale. Un prodigio della tecnica: al termine della trasmissione, la *mail* esiste in due punti diversi nello stesso momento, mentre la lettera viaggia da un punto all'altro sottraendo la sua disponibilità al mittente per consentirla al destinatario. Ma non sono solo le regole ad essere diverse, anche gli oggetti sono diversi. Gli oggetti informatici, anche se rappresentano nell'astratto oggetti reali, esistono solo nel mondo virtuale e seguono le regole dell'elettronica, della chimica e dell'elettromagnetismo oltre che dell'algebra, della geometria e dell'analisi matematica. Alcuni di questi oggetti, come immagini, musica, informazioni in genere e filmati, esistono addirittura solo nel mondo digitale e non hanno nessun riferimento fisico nel mondo reale.

Il mondo virtuale è, infine, un mondo totalmente interconnesso, mentre il mondo reale ha solo dei punti uniti tra loro dal territorio, dalle acque, dalle strade, dalle vie aeree e così via: tutti percorsi che seguono le regole della fisica tradizionale. Tempo e spazio, velocità e distanza sono fattori reali che seguono le regole della fisica naturale. Un omicidio per strangolamento, infatti, non può essere imputato a un soggetto che dopo solo due minuti dal fatto si trova in un altro continente, mentre

lo stesso non si può affermare per un reato informatico. Ma cosa accadrebbe se nel futuro la tecnologia ci mettesse a disposizione il teletrasporto ? Certamente dovremmo almeno ripensare le procedure di indagine e le relative norme del diritto sostanziale.

Nel mondo virtuale il reo potrebbe colpire un bene da qualsiasi luogo egli desideri, anche dallo spazio orbitale oltre la stratosfera: sarebbe sufficiente avere una connessione alla rete *internet*.

Bisogna, quindi, cambiare il nostro modo di pensare e ammettere che nel mondo virtuale possono esistere situazioni ritenute impossibili nel mondo reale, ma comunque riconducibili al mondo reale poiché il soggetto attivo è sicuramente un essere umano, penalmente perseguibile.

Ecco quindi la ragione della confusione che si sta rapidamente diffondendo in questa materia. Una confusione che nasce proprio da questa astrazione, cioè dal fatto che il luogo di consumazione del reato informatico può corrispondere a più luoghi nel mondo reale, un'idea dalla quale nasce tutta una serie di interpretazioni giuridiche diverse e in conflitto tra loro. Tuttavia, ad uno sguardo più attento, dovremo anche in questo caso convenire che la soluzione è tanto chiara quanto semplice.

Si pensi, ad esempio, al delitto di accesso abusivo ad un sistema informatico o telematico previsto dall'articolo 615-*ter* del codice penale. Tizio per accedere al sistema di Caio effettua una connessione remota attraverso la rete *internet*. Tizio opera fisicamente sul suo sistema situato nel suo scantinato in Brasile mentre il sistema di Caio è situato in Italia. Tizio, grazie alle sue capacità tecniche, elude i sistemi di protezione e, prendendo il controllo del *computer* di Caio, copia le informazioni che gli servono e prima di scollegarsi distrugge i dati di Caio. Nell'ipotesi citata si assiste a un concorso di reati: accesso abusivo, danneggiamento e furto. Accesso abusivo in quanto Tizio accede al sistema di Caio contro la volontà di quest'ultimo, tacitamente espressa dal sistema di protezione che Tizio elude. Danneggiamento perché, cancellando i dati, Tizio rende non operativo il *software* installato sul sistema di Caio. Furto perché Tizio prende possesso di informazioni di Caio e le sottrae alla disponibilità di quest'ultimo. Qual è il luogo di consumazione del delitto ? Il Brasile o l'Italia ? Allo stato attuale della giurisprudenza si direbbe che il luogo di consumazione è il Brasile poiché che tutti i comandi sono stati eseguiti da questo Paese. Tuttavia, nel momento in cui Tizio si collega al *computer* di Caio, egli unisce i due sistemi in un sistema unico che fisicamente è situato sia in Brasile che in Italia e visto che per sistema, in questo caso, dobbiamo considerare il sistema oggetto del reato, dobbiamo considerare sistema quello della vittima, che è fisicamente posto in Italia. Il luogo del reato è, quindi, certamente l'Italia.

Esaminiamo ora un altro caso. Tizio accede abusivamente alla posta elettronica di Caio. La casella di posta elettronica di Caio è una casella *gmail* digitalmente custodita non sul *computer* di Caio ma sui *server* americani di Google. Quale il luogo di consumazione del reato ? Il Brasile, gli USA o l'Italia ? In base alla giurisprudenza attuale si dovrebbe escludere l'Italia, facendo ricadere la scelta tra Brasile e USA, ma anche in questo caso la risposta corretta è un'altra. I luoghi nei quali è situato il sistema sono in realtà tutti e tre, distribuiti sul pianeta, ma solo uno è il luogo dove si consuma il reato. La connessione virtuale unisce fisicamente i tre luoghi distanti tra loro in un sistema unico che poggia sui tre punti tramite l'uso fisico e reale di un cavo di rete dell'infrastruttura *internet*. La rete *internet*, invece, quale portatrice di informazione e infrastruttura pubblica, non fa parte di nessuno dei tre sistemi e, quindi, deve essere esclusa la bizzarra ipotesi dell'unione di tutti punti di ubicazione del sistema quale spazio costituente il luogo del reato. Infatti la posta di Caio memorizzata sui *server* altro non è che una serie di dati binari elettronicamente memorizzati su un supporto di memoria che nulla hanno a che vedere con la funzione di posta fino al momento in cui un sistema, collegandosi, non visualizzi tali informazioni sul proprio terminale sotto

forma di testo e di immagini, dando a quegli impulsi elettrici la funzione di posta. Pertanto, quando Caio vuole leggere la sua *gmail* apre una connessione ovvero collega fisicamente il proprio sistema all'*hard disk* di Google, che altro non è che una periferica esterna posta a migliaia di chilometri di distanza dal *computer* di Caio e della quale Caio ha piena disponibilità. Il sistema è il dispositivo che realizza la funzione per il quale è stato costruito e, nel caso dei *computer*, la sua funzione è quella di interagire con l'utente attraverso dispositivi di *input* e di *output* quali tastiera, *monitor* e stampanti. L'*hard disk* di Google da solo non è un sistema ma una periferica e questo vale anche per Tizio. Quando Tizio si collega al *server* di Google in realtà si collega al sistema di Caio che, anche se in quel momento non risulta connesso, è comunque collegato virtualmente alla periferica che resta a sua disposizione, ma che in quel momento semplicemente non sta usando. Caio, la vittima, può accedere alla sua *gmail* da diversi luoghi: da casa, dall'ufficio, da un *hotel*, da una spiaggia o in movimento tramite il cellulare. E allora qual è il luogo dove è situato il sistema di Caio? Non potendo rispondere « dovunque », si può convenire che il sistema di Caio, in quanto estensione nel mondo virtuale del domicilio tradizionale, è situato esattamente dove Caio ha il proprio domicilio tra il momento del fatto e il momento in cui viene a conoscenza del fatto in funzione della fattispecie in questione. Ecco quindi che Il domicilio virtuale segue la persona fisica ovunque essa sia ovvero ovunque essa abbia eletto il proprio domicilio al momento del fatto, come d'altronde accade nella realtà. Nel caso della persona giuridica, il domicilio deve certamente coincidere con la sede legale e operativa.

In conclusione, nel caso di un reato informatico lo spazio di esecuzione del reato è rappresentato dai luoghi fisici dove sono situati tutti i dispositivi utilizzati dal reo e tutti quelli facenti parte del sistema della vittima o del suo sistema e di eventuali reti periferiche coinvolte, escludendo le periferiche non oggetto del reato. Il luogo di consumazione del reato è, invece, il luogo dove risiede la vittima.

In ogni caso, queste tesi, che possono essere accettate o no, garantirebbero una tutela maggiore della vittima e amplierebbero lo spazio di competenza. Tale maggiore garanzia compenserebbe, inoltre, l'infinita scelta dei luoghi dai quali il criminale potrebbe commettere il reato: praticamente qualsiasi luogo dell'universo esplorato e dello spazio orbitale satellitare nonché qualsiasi giurisdizione. Questo non è certamente attuabile nel mondo reale ed è il motivo per cui bisogna adattare il pensiero giuridico alle nuove frontiere che vanno oltre il tradizionale modo di pensare la realtà.

PROPOSTA DI LEGGE

—

Art. 1.

(Modifiche all'articolo 61 del codice penale, in materia di circostanze aggravanti comuni per i reati commessi attraverso strumenti informatici o telematici)

1. All'articolo 61 del codice penale sono aggiunti, in fine, i seguenti numeri:

« 11-*octies*) l'aver utilizzato un sistema informatico o telematico come strumento di perpetrazione del reato;

11-*novies*) nei reati compiuti attraverso strumenti informatici o telematici:

11-*novies*.1) l'avere agito con particolare abilità tecnica ovvero utilizzando programmi o dispositivi informatici o telematici diretti ad accedere abusivamente, a danneggiare o a interrompere un sistema informatico o telematico;

11-*novies*.2) l'avere agito utilizzando programmi o dispositivi informatici o telematici diretti a occultare l'identità digitale o l'indirizzo di rete del dispositivo utilizzato per compiere il reato;

11-*novies*.3) l'avere agito sottraendo l'identità digitale di terzi;

11-*novies*.4) l'avere agito alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico ovvero intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti;

11-*novies*.5) l'avere agito abusando della conoscenza del codice sorgente del dispositivo informatico o telematico oggetto del reato ovvero l'avere agito in qualità di produttore del sistema informatico o telematico oggetto del reato;

11-*novies*.6) l'avere agito per il tramite di un sistema di posta elettronica, di un sistema di messaggistica, di dispositivi

telefonici ovvero di qualsiasi sistema di conversazione informatica o telematica;

11-*novies*.7) l'avere agito con dispositivi informatici o telematici aventi una grande potenza di calcolo ».

Art. 2.

*(Introduzione dell'articolo 10-*bis *del codice di procedura penale, in materia di competenza per i reati commessi attraverso strumenti informatici o telematici)*

1. Dopo l'articolo 10 del codice di procedura penale è inserito il seguente:

« Art. 10-*bis*. – *(Competenza per i reati commessi attraverso strumenti informatici o telematici) – 1.* Se il reato è stato commesso attraverso strumenti informatici o telematici, la competenza è determinata dal luogo di residenza, domicilio o dimora abituale della persona offesa ovvero, qualora il reato sia stato commesso in danno di una persona giuridica, dal luogo della sede legale di questa ».

18PDL0090440