Poliziamoderna

Crimini con i bit

Introduzione Con la legge 23 dicembre 1993, n. 547 “Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”, il legislatore ha, per la prima volta, messo mano organicamente alla materia dei reati informatici. Scelta la via della novellazione con un vasto intervento all’interno del corpus codicistico (sostanziale e, in minor parte, anche processuale), proprio al fine di evitare le dispersioni proprie di quello che poteva anche diventare una sorta di “testo unico” (peraltro, in un quadro già ben noto di iperproduzione legislativa), il legislatore ha inteso normare soltanto in tema di reati informatici o telematici propri. Può, infatti, dirsi definitivamente acquisita la giustapposizione tra reati commessi su beni informatici e telematici (appunto, reati informatici e telematici “propri”) e reati commessi mediante beni informatici o telematici (reati informatici e telematici “impropri”), focalizzante con precisione l’oggetto delle tutela. Tale scelta, pur con un paio di sbavature, è stata, infine, confermata con la legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della convenzione di Budapest del 2001 sulla criminalità informatica, occasione che ha consentito al nostro legislatore anche di affinare alcune norme introdotte nel 1993 che, nel corso degli anni, avevano manifestato non pochi limiti. In questo articolo si parlerà della prima tipologia di reati. Successivamente, in un diverso articolo, sarà presentata una rassegna dei secondi concludendo con un’analisi delle norme processuali specifiche. **Il “domicilio informatico” e la sua tutela** Tecnologica estensione dell’essere umano, vera e propria “casa” proiettata nel mondo tangibile mediante strumenti informatici e telematici, il “domicilio informatico” è stato affiancato, anche con espresso ossequio all’art. 14 Cost., alla già nota figura del domicilio “fisico”. L’accostamento non emerge soltanto dai dati letterali e sistematici, ma pure dalla relazione al disegno di legge S. 2773, XI legislatura dai cui è sortita la legge 547/93. I casi di accesso abusivo telematico, che, in un linguaggio oramai acquisito, si consumano col “bucare” un sistema il cui accesso è riservato a uno o più utenti determinati, sono assai frequenti, molto più di quello che si può pensare. Ciò anche per la molteplicità dei motivi che inducono a compiere detti accessi: dall’appropriazione di informazioni riservate, a finalità vandalistiche passando anche per la mera ostentazione di capacità tecniche. L’art. 615 ter cp prevede la particolare figura dell’accesso abusivo a sistema informatico o telematico sanzionando “chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo”. Come anticipato sopra, l’inserimento, tra i delitti contro l’inviolabilità del domicilio, del reato in argomento, non è affatto casuale, sicché sarà possibile attingere alle conclusioni già consolidatesi sulle norme poste a presidio del domicilio “tradizionale”, prima fra tutte l’art. 614 cp (violazione di domicilio). Certo è, però, che le peculiarità del mondo dei bit devono sempre consigliare un’attenta interpretazione, coerente con questo settore. In termini generali, occorre sottolineare che l’accesso rilevante per la norma in esame (“locale”, vale a dire da tastiera o altro dispositivo di input, o “remoto” che sia), è soltanto quello di tipo informatico o telematico. Esulano dalla copertura della norma gli accessi fisici (ad esempio la materiale apertura del contenitore) relativamente ai quali rilevano, invece ed eventualmente, altre ipotesi di legge. Di grande importanza è la discussione riguardante le “misure di sicurezza” menzionate dalla norma incriminatrice. Di conseguenza, un sistema non protetto da dette misure non è tutelato dalla legge. Ma cosa rientra nel concetto di “misura di sicurezza”? Va premesso che si tratta di un àmbito vastissimo. E, in effetti, si va dalle semplici password al più sofisticato dei firewall passando per smartcard identificative e dispositivi di riconoscimento biometrico di caratteristiche fisiologiche (es. impronta digitale e iride) o comportamentali (es. impronta vocale). Ma siccome la misura di sicurezza ha la funzione minima di rendere esplicito e in equivoco il divieto di accesso, nella categoria potrebbe ben rientrare anche un semplice “cartello” informatico che comunichi efficacemente detto divieto (sostanzialmente su questa linea, Tribunale di Torino, sez. IV, sentenza 7 febbraio 1998, in Penale.it, http://www.penale.it/page.asp?mode=1&IDPag=91). Ciò che accomuna la specie delle misure di sicurezza è la manifestazione di volontà (esplicitata proprio con la predisposizione anche della minima misura) contraria all’intrusione o alla permanenza nel sistema. Sicché l’intrusione penalmente rilevante deve avvenire invito domino, vale a dire contro la volontà del titolare. Detto ciò, occorre porre alcuni distinguo tra sistemi informatici e sistemi telematici. Non v’è dubbio che una serratura posta sulla tastiera costituisca segno inequivocabile dell’accesso riservato. Ma tale evidenza vale soltanto per un accesso locale. La presenza di un’eventuale barriera fisica non è, infatti, assolutamente percepibile tramite Internet o mediante una connessione telematica. Considerato che il dolo deve sempre impegnare l’intero oggetto del reato, un eventuale intruso telematico inconsapevole del dispositivo “fisico” non sarebbe sanzionabile per carenza di elemento soggettivo. Come visto sopra, il legislatore ha, di fatto, imposto un onere di autotutela in capo al titolare del sistema informatico o telematico nella misura in cui questi, per invocare la giustizia penale, dovrà implementare le misure di sicurezza meglio viste. Ciò è confermato in giurisprudenza, come si

può evincere da una nota sentenza del giudice dell'udienza preliminare presso il Tribunale di Roma che ha correttamente ritenuto non punibile un accesso telematico non protetto da misure di sicurezza (giudice dell'udienza preliminare presso il Tribunale di Roma, 4 aprile 2000, in Penale.it, http://www.penale.it/giuris/meri_047.htm). Sin qui si è discusso dell'ipotesi di introduzione prevista dalla norma; quest'ultima, però, sanziona (peraltro in modo del tutto analogo a quanto disposto per la violazione di domicilio ex art. 614 cp), anche i casi di permanenza nel sistema, divenuta illecita successivamente all'accesso, vale a dire a seguito della revoca dell'autorizzazione oppure, secondo alcuni, col compimento di azioni diverse da quelle per cui era stato permesso l'accesso. Come appena osservato, non è universalmente condivisa la sanzionabilità, secondo la norma in esame, di chi, ad esempio (ma si tratta di casi giudiziari reali), pur essendo abilitato all'accesso a una banca dati (quella in uso alle forze dell'ordine oppure il registro degli indagati di una certa procura, ecc.) l'ha consultata per fini estranei alle proprie mansioni. Così, in un caso, la giurisprudenza di merito ha affermato che l'impiegato dell'Agenzia delle Entrate che acceda e si intrattenga nel sistema informatico per pochi secondi e per finalità diverse per le quali vale la sua autorizzazione o per visionare dei soli dati anagrafici non commette il reato di cui all'art. 615 ter cp per esclusione dell'elemento soggettivo (giudice dell'udienza preliminare presso il Tribunale penale di Nola, sentenza 11 dic

...

01/11/2010