

ATTENTATO AD IMPIANTI INFORMATICI E TELEMATICI DI PUBBLICA

UTILITÀ

L'art. 2 della legge 547/93 ha sostituito per intero l'art. 420 c.p. allo scopo di *“estendere la tutela penale apprestata dalla norma, sia nell'ipotesi base del delitto nella stessa previsto, che in quella circostanziata, ai sistemi informatici o telematici, nonché ai dati, alle informazioni o ai programmi in essi contenuti.”*¹

La riformulazione dell'art. 420 c.p. si è resa necessaria per poter chiarire i numerosi dubbi interpretativi insorti rispetto al precedente tenore della norma, che puniva gli autori di *“un fatto diretto a danneggiare o distruggere impianti di pubblica utilità o di ricerca o di elaborazione dati”*.

La formulazione, chiaramente alternativa, della norma aveva fatto ritenere che il delitto in questione fosse ravvisabile anche per i casi in cui la condotta si rivolgesse contro impianti di ricerca o di elaborazione dati, a prescindere dalla loro pubblica utilità. Inoltre, risultava incerta la stessa possibilità di tutelare dati, programmi e informazioni.

In particolare, ampia parte della dottrina criticò aspramente una pronuncia del giudice istruttore di Firenze, che ritenne applicabile il

¹ Cfr. Relazione introduttiva al disegno di legge

vecchio testo dell'art. 420 c.p. ad una condotta avente ad oggetto il solo software, quindi senza alcuna lesione alla componente hardware dell'impianto².

Per evitare tali problemi, il legislatore ha opportunamente riformulato l'art. 420 c.p. Più in particolare, il primo comma non presenta più il riferimento agli impianti di ricerca o elaborazione dati, per il resto mantenendosi come reato a consumazione anticipata, *“il cui momento realizzativo coincide con il porre in essere l'azione diretta a danneggiare o distruggere”*³ l'impianto di pubblica utilità.

La relazione introduttiva alla legge precisa, ai fini della configurabilità del delitto in parola, che per impianti di pubblica utilità si deve intendere un insieme di strutture e apparecchi che, pur appartenendo ai privati, abbiano un tale rilievo sociale che una condotta diretta a danneggiarli non può lasciare indifferente la collettività.

Tale nozione di pubblica utilità ricalca, peraltro, quella accolta in numerose sentenze dalla Corte di Cassazione⁴.

Da quanto detto emerge con sufficiente chiarezza che il bene tutelato è rappresentato dalla *“regolarità del funzionamento”*⁵ degli impianti di

² Borruso-D'Aiotti AA.VV. *op. cit.*, pag. 61.

³ Cfr. Relazione introduttiva al disegno di legge

⁴ Per tutte si veda, Cass. 21/4/1980 in *Giurisprudenza italiana*, 1981, II, pag. 371.

⁵ Borruso-D'Aiotti AA.VV. *op. cit.*, pag. 63.

pubblica utilità, a prescindere dalla distruzione o dal danneggiamento degli stessi.

Il secondo comma, invece, aggiunge una specifica ipotesi delittuosa posta a tutela dei sistemi informatici e telematici di pubblica utilità.

Ancora una volta si deve apprezzare la scelta del legislatore, che ha previsto espressamente la punibilità dell'azione diretta al danneggiamento o alla distruzione di un sistema informatico o telematico, e soprattutto di quella rivolta contro i dati, le informazioni o i programmi, così evitando qualsiasi dubbio in ordine alla violazione del precetto di cui all'art. 14 delle disposizioni sulla legge in generale.

Nel terzo comma, infine, è prevista un'unica circostanza aggravante se dai fatti di cui al primo e al secondo comma deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, dei programmi o delle informazioni ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è aumentata (da 3 ad 8 anni di reclusione; per il delitto base, invece, la pena oscilla da 1 a 4 anni). Dunque l'aumento di pena è dovuto al verificarsi di un evento ulteriore rispetto ad un fatto base che già costituisce un reato: si tratta quindi, di un reato aggravato o qualificato dall'evento⁶.

⁶ Cfr. Fiandaca-Musco *op. ult. cit.*, pag. 480.

Come ha osservato un'attenta dottrina, il legislatore non è però intervenuto su di una norma del codice penale che “è rivolta alla tutela di un bene del tutto affine a quello tutelato dall'art. 420 c.p.”⁷, cioè l'art.433 c. p. (*Attentati alla sicurezza degli impianti di energia elettrica e del gas ovvero delle pubbliche comunicazioni*); esso prevede infatti, al secondo comma, la punibilità di chi “attenta alla sicurezza delle pubbliche comunicazioni... qualora dal fatto derivi pericolo per la pubblica incolumità”.

Vero è pure, tuttavia, che poiché l'art. 623 -bis (*altre comunicazioni e conversazioni*) equipara, *in toto*, le comunicazioni e le conversazioni telegrafiche e telefoniche a quelle informatiche, si potrebbe propendere per una interpretazione estensiva dell'art. 433 c.p., per le ipotesi in cui gli “attentati” coinvolgono comunicazioni informatiche e telematiche.

Queste ultime costituiscono, a ben vedere, solo una mera evoluzione tecnologica di quelle forme di comunicazione che il legislatore del 1930 aveva inteso tutelare.

Una tale opzione ermeneutica non ricade nel divieto di applicazione analogica della legge penale, poiché rientra nell'ambito dei possibili significati letterali impiegati nel testo di legge.

⁷ Borruso-D'Aiotti AA.VV. *op. cit.*, pag. 64.

