L’accesso *“abusivo”* ad un sistema informatico o telematico.

Riflessioni e considerazioni alla luce delle evoluzioni giurisprudenziali della Corte di Cassazione

*E’ sbagliato usare mezzi immorali per raggiungere fini morali. Ma ora devo affermare che è altrettanto sbagliato utilizzare mezzi morali per raggiungere fini immorali (Martin Luther King)*

Partendo dall’aforisma di Martin Luther King, prima di analizzare la fattispecie penale in argomento, occorrerebbe, forse, spostare il nostro punto di osservazione rispetto all’oggetto osservato, ovvero, potrebbe risultare utile ricordarsi per quale motivo si dispone di un qualunque mezzo, di un qualunque strumento fornito quale ausilio al fine di un migliore raggiungimento di determinati scopi, così da assolvere efficientemente e celermente i compiti demandati.

La banca dati in uso alle Forze di Polizia (S.D.I.), al pari dei più recenti portali (Hydra, Infocamere, AGweb, Anagrafe Comune, etc, ), è uno strumento utilissimo, ormai divenuto quasi indispensabile poiché fonte di informazioni fondamentali alle attività di indagine ed istituzionali in genere; E’ proprio per questo motivo che vige una rigida normativa di accesso ed utilizzo, con i relativi risvolti di natura penale, oltre che disciplinari.

Quando, dal punto di vista dottrinale e giurisprudenziale, l’accesso è da considerarsi *“abusivo”* ? Quale elemento della condotta qualifica *“l’abusività”* di un accesso?

Sul punto, occorre preliminarmente segnalare l’evoluzione giurisprudenziale relativa alla corretta qualificazione giuridica della condotta del soggetto attivo, in funzione della quale si è ritenuto che la stessa integrasse – o meno – quella sanzionata dall’art 615 ter del codice penale.

Tale evoluzione è partita dalla considerazione della fattispecie in argomento, in analogia con quella di cui alla violazione di domicilio (art. 614 c.p. violazione di domicilio; art. 615 c.p. violazione di domicilio commessa dal pubblico ufficiale).

La Suprema Corte, con la sentenza n.12732 del 07/11/2000 aveva già argomentato in tal senso: *“l’analogia con la fattispecie della violazione di domicilio deve indurre a concludere che integri la fattispecie criminosa [prevista dall’art. 615‐ter cod. pen.] anche chi, autorizzato all’accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l’accesso. Infatti, se l’accesso richiede un’autorizzazione e questa è destinata a un determinato scopo, l’utilizzazione dell’auto****r****izzazione per uno scopo diverso non può non considerarsi abusiva”.*

Infatti, il citato art. 615 ter (introdotto con la legge 23 dicembre 1993 n. 547), sanziona al primo comma l’introduzione abusiva ad un sistema informatico o telematico protetto da misure di sicurezza ( l’attività compiuta dal c.d. hacker o pirata informatico) ed al secondo comma *“anche quella del soggetto abilitato all’accesso, e perciò titolare di un codice d’ingresso, che s’introduca legittimamente nel sistema, per finalità però diverse da quelle delimitate specificamente dalla sua funzione e dagli scopi per i quali la password gli è stata assegnata”.[[1]](#footnote-1)*

Ne consegue che, il Pubblico Ufficiale, autorizzato all’accesso alle Banche Dati in uso alle Forze di Polizia per l’espletamento delle funzioni a lui demandate per motivi di sicurezza, di ordine pubblico, per ragioni connesse alle indagini di P.G., sebbene in possesso di autorizzazioni (userid e password), acceda alle predette banche dati per fini diversi, è da considerare alla stregua di chi vi accede in modo “*abusivo*”.

Tale orientamento ha come fondamento la considerazione che la norma in esame, come già detto, non punisce esclusivamente l’accesso abusivo nel sistema da parte di chi non avrebbe comunque titolo ad accedervi, **ma anche la permanenza nel sistema contro la volontà di chi ha il diritto di escluderla**. Tale volontà è da considerarsi **tacitamente contraria** nel caso in cui il soggetto persegua finalità illecite e quindi incompatibili con le ragioni per le quali l’autorizzazione all’accesso al sistema era stato concesso: Ecco che l’accesso diviene abusivo!

Con la citata sentenza[[2]](#footnote-2) emessa dalle Sezione Unite, la Corte di Cassazione è oltremodo esaustiva sul punto e la valutazione non può prestarsi ad alcun errore interpretativo: *“Se il titolo di legittimazione all’accesso viene utilizzato dall’agente* ***per finalità diverse da quelle consentite****, dovrebbe ritenersi che* ***la permanenza nel sistema informatico avvenga contro la volontà del titolare del diritto di esclusione****. Pertanto* ***commette reato anche chi, dopo essere entrato legittimamente in un sistema, continui ad operare o a servirsi di esso oltre i limiti prefissati dal titolare****; in tale ipotesi ciò che* ***si punisce è l’uso dell’elaboratore avvenuto con modalità non consentite, più che l’accesso ad esso****”*.

Quanto sopra era già stato enunciato chiaramente nelle sentenze Bassani[[3]](#footnote-3) e Lesce[[4]](#footnote-4), le quali hanno chiarito che l’art. 615 ter c.p. *“sanziona non soltanto l’introduzione abusiva in un sistema informatico protetto, ma anche il mantenersi al suo interno – contro la volontà espressa o tacita di chi abbia il diritto di escluderlo – da parte di soggetto abilitato, il cui accesso, di per sé legittimo, diviene abusivo, e perciò illecito, per il suo protrarsi all’interno del sistema per fini e ragioni estranee a quelle d’istituto”[[5]](#footnote-5).*

Si richiama, in proposito, il citato parallelismo in analogia con la fattispecie di cui all’art. 614 c.p. (violazione di domicilio), che al comma 2° cita : *“ alla stessa pena soggiace chi si trattiene nei detti luoghi contro l’espressa volontà di chi ha il diritto di escluderlo, ovvero s’introduce clandestinamente o con inganno”* .

L’evoluzione giurisprudenziale alla quale si è fatto riferimento, ha fatto perno attorno al significato che nel tempo è stato dato al termine *“abusivo”*, sia che la fattispecie riguardasse il primo comma del citato art. 615 ter, quanto per il secondo comma dello stesso articolo.

Infatti, con numerose precedenti sentenze della medesima Suprema Corte[[6]](#footnote-6) (senza volerci addentrare troppo in questa sede nelle motivazioni delle stesse) si è ritenuto che integrasse la condotta di cui all’art. 615 ter c.p., ovvero che l’accesso fosse da considerarsi “abusivo”, **solo se effettuato da soggetto non abilitato** (soggetto estraneo, privo di userid e password).

Di converso, veniva considerato **sempre e comunque** “lecito” l’accesso effettuato da un soggetto abilitato, nonostante la valutazione *ex post* delle finalità, si rivelasse estranea a quelle d’ufficio (sentenza Peparaio) o perfino illecita (sentenza Scimia).

Il cambio di passo è stato segnato con la citata sentenza n. 4694 del 27 ottobre 2011, emanata dalla Suprema Corte a Sezione Unite, in risoluzione del contrasto giurisprudenziale sopra delineato e proprio il Collegio della Quinta Sezione aveva rimesso i ricorsi sul seguente quesito: *“se integri la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto abilitato ma per scopi o finalità estranei a quelli per i quali la facoltà di accesso gli è stata attribuita”.*

Le considerazioni in punto di diritto esaminate nella citata sentenza (alla quale si rimanda per una più completa comprensione), partono dall’analisi dei precetti contemplati nei due commi dell’art. 615 ter c.p.:

1. L’introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza (attività tipica dell’hacker)
2. Il mantenersi nel sistema contro la volontà, espressa o tacita, di chi ha il diritto di esclusione.

Questa seconda ipotesi è quella sulla quale maggiormente poniamo il nostro *focus*: Si tratta della tipica condotta posta in essere da chi autorizzato all’accesso – per determinate operazioni – si trattiene all’interno del sistema, ovvero persiste nell’avvenuta introduzione *“continuando ad accedere alla conoscenza dei dati nonostante il divieto, anche tacito, del titolare del sistema”*.

Quindi il soggetto, *“****compiuta l’operazione espressamente consentita, si intrattenga nel sistema per la presa di conoscenza, non autorizzata, dei dati****”*.[[7]](#footnote-7)

Infatti, non può prescindersi dalle finalità per le quali si dispone di un delicatissimo strumento quale, ad esempio, la Banca Dati della Forze di Polizia ed è proprio in virtù del conseguimento delle stesse che il titolare del sistema, di cui legittimamente dispone, consente l’accesso. Ne consegue che *“se il titolo di legittimazione all’accesso viene dall’agente utilizzato per finalità diverse da quelle consentite, non vi è dubbio che si configuri il delitto in discussione, dovendosi ritenere che* ***il permanere nel sistema per scopi diversi da quelli previsti avvenga contro la volontà, che può, per disposizione di legge, anche essere tacita, del titolare del diritto di esclusione****»* [[8]](#footnote-8).

Ancora, nella citata sentenza si riporta una precedente pronuncia[[9]](#footnote-9) espressa in relazione ad un accordo preventivo verificatosi tra il titolare di un’agenzia di investigazioni private ed un pubblico ufficiale che, **dietro compenso**, aveva effettuato l’accesso ad un sistema telematico o informatico (pur avendone titolo formale e quindi legittimato all’accesso) al fine di carpire e riferire notizie riservate d’interesse per l’agenzia: poiché il contesto in esame è quello di una corruzione propria, l’accesso del pubblico ufficiale è palesemente finalizzato al compimento di un atto contrario ai doveri del proprio ufficio (art. 319 c.p.), quindi l’accesso stesso diviene di per sé *“abusivo”* poiché effettuato al di fuori dei doveri del proprio ufficio ed a seguito dell’accordo criminoso di cui sopra, a prescindere dalla permanenza all’interno del sistema, contro la volontà di chi ha il diritto di escluderlo. Tale condotta configurerebbe il reato di cui all’art. 615 ter, in parola.

Sul punto, la considerazione effettuata dalla Suprema Corte è oltremodo chiarificatrice dell’ineccepibile ragionamento interpretativo sotteso: “*tanto* [ovvero la condotta di cui sopra] *sposta l’attenzione dal momento della permanenza nel sistema contro la volontà di chi ha il diritto di escluderlo, a quello dell’accesso ed è lo stesso atto di accesso a qualificarsi come integrativo del reato, a prescindere dal prosieguo della condotta»* [[10]](#footnote-10)*.*

Come già detto, in precedenza, la stessa Corte aveva adottato un’interpretazione più restrittiva del concetto di “*abusivo*” ; infatti, sempre la Quinta Sezione con la sentenza n. 2534 del 20/12/2007 (dep. 2008, Migliazzo), aveva affermato che *“non integra il reato di accesso abusivo ad un sistema informatico (art. 615‐ter cod. pen.) la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all’Arma dei Carabinieri, si introducano nel sistema denominato S.D.I. (banca dati interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all’accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi ad una agenzia investigativa, condotta quest’ultima ipoteticamente sanzionabile per altro e diverso titolo di reato”*.

Anche successive sentenze di quegli anni[[11]](#footnote-11) hanno interpretato il concetto di abusività in senso oggettivo, con esclusivo riferimento al momento dell’accesso al sistema, valutando le sole modalità (e non i fini) utilizzate per accedere, ovvero su come siano state neutralizzate e superate le misure di sicurezza (password). Secondo tale orientamento la finalità dell’accesso integrerebbe eventualmente altri differenti titoli di reato.

Con la sentenza n. 4694 in esame[[12]](#footnote-12), la Corte di Cassazione non ha analizzato la fattispecie alla sola luce delle modalità di accesso di cui sopra (concetto di abusività in senso oggettivo), né esclusivamente in riferimento alle sole finalità, quanto, piuttosto *“deve ritenersi, perciò, il profilo oggettivo dell’accesso e del trattenimento nel sistema informatico da parte di un soggetto che sostanzialmente non può ritenersi autorizzato ad accedervi ed a permanervi* ***sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema*** *(nozione specificata, da parte della dottrina, con riferimento alla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro)* ***sia allorquando ponga in essere operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato ed in relazione alle quali l’accesso era a lui consentito****”*.

Questa considerazione ci riporta alla iniziale massima di M.L. King, poiché sotto i riflettori viene posto ***“il titolo legittimante”*** che consente l’accesso e la permanenza nel sistema, tenendo presente che il titolare del sistema ne consente, appunto, l’accesso e la permanenza per un uso precipuo. Più chiaramente, il dissenso tacito del titolare del sistema, *“non viene desunto dalla finalità (quale che sia) che anima la condotta dell’agente,* ***bensì dall’oggettiva violazione delle disposizioni del titolare in ordine all’uso del sistema***”. I successivi fatti, le condotte successive all’accesso o alla permanenza, se ritenuti illeciti, andranno a configurare eventuali singoli titoli di reato (ad esempio, rivelazione di segreto d’ufficio).

Da tali considerazioni, trasponendole su piano pratico, ne consegue che un operatore che accede ad un sistema informatico o telematico in modo assolutamente legittimo (ad esempio, nel corso di una indagine in atto, effettua un’interrogazione con l’applicativo S.D.I. sul conto degli indagati o dei soggetti loro vicini) ed acquisisce delle notizie o delle informazioni delle quali successivamente ne fa un uso illecito (le rivela agli interessati o a terzi), non integra con tale condotta il reato di cui all’art. 615 ter c.p., quanto, piuttosto, altre fattispecie penali (es. rilevazione di segreto d’ufficio, di segreto istruttorio, corruzione per atti contrari ai doveri d’ufficio, etc), poiché lo stesso ha avuto accesso al sistema - ed ivi si è trattenuto - nei limiti e nelle forme consentite dal titolare (il suo accesso e le interrogazioni erano giustificate dall’indagine in corso sui soggetti indagati).

Infatti, *“Il giudizio circa l’esistenza del dissenso del dominus loci* [“il signore del luogo”, ovvero, il titolare del sistema] *deve assumere come parametro la sussistenza o meno di un’obiettiva violazione, da parte dell’agente, delle prescrizioni impartite dal dominus stesso circa l’uso del sistema* ***e non può essere formulato unicamente in base alla direzione finalistica della condotta****, soggettivamente intesa”* [[13]](#footnote-13)*.*

Le Sezioni Unite, dopo aver dipanato le considerazioni sopra riportate, concludono affermando che: *“integra la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall’art. 615‐ter cod. pen., la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto che, pure essendo abilitato, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l’accesso. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l’ingresso al sistema”.*

Anche dopo la sentenza del 2011, la Corte di Cassazione - nella sua composizione più autorevole - si è recentemente[[14]](#footnote-14) pronunciata a seguito dell’ordinanza di rimessione della Quinta Sezione Penale[[15]](#footnote-15), ribadendo il principio di diritto già precedentemente enunciato[[16]](#footnote-16) dalla stessa Corte, ovvero che : “integra il delitto previsto dall’art. 615 ter, secondo comma, n. 1, cod. pen. la condotta del pubblico ufficiale o dell’incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l’accesso, acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita”.

La questione in esame è stata talmente dibattuta (e purtroppo anche troppo frequentemente) che è divenuta nel tempo oggetto di numerose sentenze da parte della citata Corte che ha anche inquadrato la condotta tipica in esame, nell’alveo del c.d. *“sviamento di potere”*, concetto sul quale vale la pena, in questa sede, soffermarsi seppur brevemente:

Lo sviamento di potere rientra nella categoria (di ambito amministrativo) più generale del *“vizio di eccesso di potere”*, ricorrente allorquando, **nella propria attività, il pubblico ufficiale** “persegua una finalità diversa da quella che gli assegna in astratto la legge sul procedimento amministrativo”.[[17]](#footnote-17)

Anche dal punto di vista del diritto amministrativo, il pubblico Ufficiale che accede ad un sistema informatico o telematico ed acquisisce delle informazioni importanti per questioni personali (es. per il perseguimento di un interesse privato) oppure carpisce delle notizie sul conto di terzi a cui poi le rivela (favoreggiamento, indebito vantaggio nei cui confronti di soggetti sottoposti ad indagini o procedimenti penali), utilizza in modo **abusivo il sistema**, poiché la sua condotta è scorretta e disonesta nei confronti della Pubblica Amministrazione, ovvero “non ispirata ai canoni della correttezza e della lealtà, siccome ontologicamente incompatibile e diversa rispetto a quelle per le quali, soltanto la facoltà di accesso le era attribuita”. [[18]](#footnote-18)

La citata Sentenza del 2017, in merito recita testualmente : “integra il delitto previsto dall’art. 615 ter, secondo comma, n. 1, cod. pen. la condotta del pubblico ufficiale o dell’incaricato di un pubblico servizio che, pur essendo abilitato e pur non violando le prescrizioni formali impartite dal titolare di un sistema informatico o telematico protetto per delimitarne l’accesso (nella specie, Registro delle notizie di reato Re.Ge.) acceda o si mantenga nel sistema per ragioni ontologicamente estranee e comunque diverse rispetto a quelle per le quali, soltanto, la facoltà di accesso gli è attribuita”. [[19]](#footnote-19)

***Alcune riflessioni e considerazioni finali:***

Ormai nel 2020, oltre 200 anni dopo la fondazione della nostra Istituzione, in un contesto sociale sempre più connesso, integrato, ipertecnologico, dove si discute quotidianamente del contrasto e del bilanciamento tra la necessità di tutelare i dati e le informazioni personali (la c.d. tutela della privacy) e l’irrinunciabile bisogno di acquisire e disporre degli stessi dati per la tutela dell’ordine e della sicurezza pubblica, l’operatore di polizia 4.0 (ormai, da anni, si parla della quarta rivoluzione industriale, di industria 4.0) non può vivere ed operare avulso dal contesto che lo circonda, dalle insidie che si celano dietro l’uso errato ed improprio **di tutti** gli strumenti di cui ha la disponibilità.

Il citato operatore, non può non conoscere le conseguenze che potenzialmente possono scaturire da un uso scorretto dei sistemi informatici e telematici messi a disposizione. A tal proposito, non si pensi soltanto al più volte citato S.D.I., poiché le stesse disposizioni di legge, le considerazioni delle sentenze citate, **si applicano a tutti i sistemi telematici ed informatici di cui si dispone** (anagrafe tributaria, anagrafe civile, sistemi delle società telefoniche, intestatari delle utenze, etc).

Potrebbe risultare utile adeguare la propria mentalità investigativa, il proprio approccio rispetto ai mezzi informatici a disposizione (ed a tutti i mezzi in generale), in funzione delle finalità per le quali sono forniti e quali sono i presupposti, le *“regole di ingaggio”* per poterli utilizzare:

* Mi serve acquisire un determinato dato per un’attività di indagine in corso? Sono legittimato ad acquisirlo? Allora acquisisco il dato secondo le modalità previste dalla legge e dai regolamenti, secondo le procedure previste per l’utilizzo di quel sistema telematico o informatico, lascio traccia nei relativi ed eventuali registri. Sarò così nelle condizioni di poter sempre motivare e giustificare l’accesso e la permanenza nel sistema telematico ed il reperimento delle informazioni che sono confluite nella citata attivata d’indagine già esistente;
* Non è ancora in corso un’attività di indagine, ma ho necessità di acquisire un determinato dato dal quale potrebbe scaturire una potenziale attività investigativa? Allora io, operatore 4.0, preparato, professionale e capace, creo le circostanze che giustificano l’utilizzo di quel mezzo. Perché i mezzi sono dati per assolvere un compito e devono essere utilizzati. Come?

Quanti, acquisita una determinata notizia confidenziale, una potenziale notizia di reato contenente nomi e cognomi, luoghi, targhe, soprannomi, **prima di effettuare una qualunque interrogazione**, redigono una relazione di servizio, una annotazione di P.G., lasciano traccia con un qualunque atto prodromico all’accertamento stesso?

Una volta redatta la relazione di servizio, la si pone all’attenzione del proprio comandante, del proprio superiore gerarchico (visto, protocollo, classificazione, ect) e dopo aver discusso dell’intenzione di volere approfondire – anche attraverso l’utilizzo di un sistema telematico o informatico – si è più che legittimati all’accesso, alla permanenza, al reperimento delle relative informazioni (sui quali esiti è doveroso sempre relazionare a completamento dell’iter avviato con la propria relazione).

Credo sia superfluo precisare che nei casi di necessità ed urgenza, dando per scontati i presupposti sopra indicati (l’esistenza di un’attività di indagine o l’assoluta necessità di acquisire un dato per un’attività in itinere della quale, comunque, immediatamente dopo si riferirà per iscritto), l’accesso e la permanenza ai sistemi telematici è comunque giustificato per i motivi sopra esposti, avendo sempre l’accortezza di relazionare ed informare immediatamente dopo su tutte le attività compiute, compresi gli accertamenti.

Sul punto, prendendo ad esempio l’applicativo S.D.I., la schermata iniziale di accesso al sistema ci viene incontro ed è stata ideata proprio per aiutarci: si ha la disponibilità di un campo libero sul quale scrivere i motivi (a futura memoria) che ci hanno indotto a ricorrere al sistema telematico medesimo: Attività di indagine? Numero di Pratica? Numero del Procedimento Penale? Altro?

Viene data la possibilità all’operatore di sintetizzare le motivazioni che giustificano “*la condotta di accesso o di mantenimento nel sistema posta in essere da soggetto”* al fine di dimostrare che non si stanno violando  *“le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l’accesso”.*

Se si fanno due conti, al netto delle brevissime (e sicuramente incomplete) considerazioni sopra riportate, resterebbero soltanto gli accessi ingiustificati, immotivati, quelli che hanno già in radice un improprio consapevole utilizzo del sistema, se non peggio la commissione volontaria di un reato.

*Mi dici chi è questo ragazzo che frequenta mia figlia? Vorrei affittare una casa, ma chi sono questi soggetti? Arrivano continui squilli a mia moglie, mi dici a chi è intestata questa utenza? Ho avuto un incidente e il Tizio è scappato, posso darti una targa? Ma quel tale è in regola o lavora in nero?*

Sono solo alcuni banalissimi esempi di come l’utilizzo del mezzo telematico non potrà mai essere giustificato né dalle motivazioni alla base dell’accesso, né dalle finalità dell’utilizzo e men che meno, questi presupposti, potranno mai rispettare *“le* *prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l’accesso”.*

Il *“giro losco”* di motorini al parco sotto casa, il *“via vai”* di macchine nei pressi di un’abitazione di cui si ha conoscenza, qualunque “scintilla” di una potenziale indagine, sebbene agli albori, troverà la sua **unica** collocazione dentro una relazione di servizio, una annotazione firmata e depositata - discussa con il proprio comandante - in virtù della quale tutti gli accessi, le interrogazioni e accertamenti successivi a qualunque applicativo informatico e telematico (di cui, come detto, si dovrà lasciare traccia), risulteranno giustificate e/o comunque motivate. E’ solo una questione di mentalità. Queste considerazioni non devono essere viste come uno scoglio o un limite al nostro operato, bensì rappresentano una tutela, una garanzia per l’operatore che sarà così in grado di spiegare – anche dopo molto tempo – le motivazioni alla base del proprio operato.

In ultimo, non dimentichiamo che, come già detto, l’utilizzo successivo delle informazioni indebitamente acquisite ed illegalmente divulgate[[20]](#footnote-20), integrerà singoli fattispecie di reato (es., rivelazione di segreto d’ufficio, favoreggiamento, rivelazione di segreto istruttorio, abuso d’ufficio, etc) e la *qualità* rivestita di Pubblico Ufficiale, di operatore di polizia, costituirà una fattispecie aggravata ed espressamente prevista, poiché se da una parte il reato in parola è un reato comune (ovvero, il soggetto attivo può essere chiunque), dall’altra, il comma 2 n. 1 dell’art. 615 ter, è stato *cucito* appositamente sul Pubblico Ufficiale, ed infatti cita testualmente:

La pena è della reclusione **da uno a cinque anni**:

1. se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

|  |  |
| --- | --- |
|  | *Arturo Davide*  *Villagrasso* |

Alcuni riferimenti normativi citati:

* Legge 1 aprile 1981, n. 121;
* art. 1, legge n. 241 del 1990
* Legge 23 dicembre 1993 n. 547;
* Artt. 81, comma secondo, e 615‐ter, comma secondo n. 1 e comma terzo c.p.;
* Corte di cassazione, Sez. 5 n.12732 del 07/11/2000, Zara;
* Corte di cassazione, Sez. 5 n. 37322 del 08/07/2008, Bassani;
* Corte di cassazione, Sez. 5, n. 1727 del 30/09/2008, dep. 2009, Romano;
* Corte di cassazione, Sez. 5 n. 18006 del 13/02/2009, Russo;
* Corte di cassazione, Sez. 5 n. 2987 del 10/12/ 2009, Matassich;
* Corte di cassazione, Sez. 5 n. 19463 del 16/02/2010, Jovanovic;
* Corte di cassazione, Sez. 5 n. 39620 del 22/09/2010, Lesce;
* Cass. pen., Sez. un., ud. 27 ottobre 2011 (dep. 7 febbraio 2012), n. 4694 Pres. Lupo, Rel. Fiale, ric. C. e altri
* **Corte di Cassazione - Sezione Quinta Penale, Sentenza 12 gennaio 2018, n. 1021**
* Ordinanza 14 marzo 2017, n. 12264
* Sezioni Unite, Sentenza 8 settembre 2017, n. 41210
* legge 1° aprile 1981, n. 121 “*Nuovo ordinamento dell’amministrazione della Pubblica Sicurezza*” (artt.5-6-7-8-9-10-11-12);
* D.P.R. 3 Maggio 1982, n.378 in relazione all’art.8 della Legge 121/81;
* legge 31 dicembre 1996, n. 675 “*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*”;
* D.Lgs. 30.6.2003, n. 196 “*Codice in materia di protezione dei dati Personali*;
* legge 26 marzo 2001, n. 128 “*Interventi legislativi in materia di tutela della sicurezza dei cittadini*” (pacchetto sicurezza);
* Decreto legge 31 marzo 2005, n. 45 “*Disposizioni urgenti per la funzionalità dell’Amministrazione della Pubblica Sicurezza, delle Forze di Polizia e del Corpo Nazionale dei Vigili del Fuoco*”

1. Cass. pen., Sez. un., ud. 27 ottobre 2011 (dep. 7 febbraio 2012), n. 4694 Pres. Lupo, Rel. Fiale, ric. C. e altri [↑](#footnote-ref-1)
2. Ibidem nota 1 [↑](#footnote-ref-2)
3. Corte di cassazione, Sez. 5 n. 37322 del 08/07/2008, Bassani; [↑](#footnote-ref-3)
4. Corte di cassazione, Sez. 5 n. 39620 del 22/09/2010, Lesce; [↑](#footnote-ref-4)
5. Ibidem nota 1 [↑](#footnote-ref-5)
6. Sentenze Migliazzo (Sez. 5, n. 2534 del 20/12/2007), Scimia (Sez. 5, n. 26797 del 29/05/2008), Peparaio (Sez. 6, n. 3290 del 08/10/2008), Genchi (Sez. 5, n. 40078 del 25/06/2009). [↑](#footnote-ref-6)
7. Ibidem nota 1 [↑](#footnote-ref-7)
8. Ibidem nota 1 [↑](#footnote-ref-8)
9. Sentenza n. 19463 del 16/02/2010, Jovanovic, riportata e commentata nella già citata sentenza n. 4694 Pres. Lupo, Rel. Fiale, ric. C. e altri [↑](#footnote-ref-9)
10. Ibidem nota 10 [↑](#footnote-ref-10)
11. Quinta Sezione con la sentenza n. 26797 del 29/05/2008, Scimia; Sesta Sezione, con la sentenza n. 39290 del 08/10/2008, Peparaio; L’indirizzo in esame è stato seguito poi dalla Quinta Sezione con la sentenza n. 40078 del 25/06/2009, Genchi. [↑](#footnote-ref-11)
12. Ibidem nota 1 [↑](#footnote-ref-12)
13. Ibidem nota 1 [↑](#footnote-ref-13)
14. **Corte di Cassazione - Sezione Quinta Penale, Sentenza 12 gennaio 2018, n. 1021** [↑](#footnote-ref-14)
15. Ordinanza 14 marzo 2017, n. 12264 [↑](#footnote-ref-15)
16. Sezioni Unite, Sentenza 8 settembre 2017, n. 41210 [↑](#footnote-ref-16)
17. art. 1, legge n. 241 del 1990 [↑](#footnote-ref-17)
18. Ibidem nota 16 [↑](#footnote-ref-18)
19. Ibidem nota 16 [↑](#footnote-ref-19)
20. Si rammenta, in merito, il divieto di stampare i risultati delle interrogazioni dell’applicativo S.D.I. *“se non nei casi di effettiva necessità e comunque previa autorizzazione da parte del comandante diretto”*. Prescrizione, questa, purtroppo sconosciuta a molti operatori. [↑](#footnote-ref-20)