UFFICIO STUDI CODAU

"Documento redatto con il contributo dei componenti dell'Ufficio Studi e VALIDATO dal Comitato Scientifico del Codau"

Accesso abusivo a sistema informatico da parte del dipendente infedele (o curioso)[1]

Sommario

Sintesi: Il dipendente pubblico, anche se formalmente autorizzato con specifiche credenziali (username e password), non può trattenersi e utilizzare i sistemi informatici istituzionali contro la volontà espressa o tacita del titolare del sistema: 1) violando le disposizioni organizzative del datore di lavoro; 2) svolgendo attività ontologicamente estranee alle ragioni di servizio. La mera violazione del c.d. domicilio informatico configura il reato di "accesso abusivo a sistema informatico o telematico" (art. 615-ter), un reato che si perfeziona senza che sia necessaria una effettiva lesione dei diritti del titolare del sistema. Sono irrilevanti, ai fini dell'integrazione del delitto, le motivazioni dell'agente, la natura dei dati contenuti nel sistema o le eventuali azioni successivamente compiute (salvo eventuali aggravanti o ulteriori reati concorrenti).
Nel caso del pubblico ufficiale o di incaricato di pubblico, lo svolgimento di operazioni ontologicamente estranee alle ragioni d'ufficio realizza un vero e proprio "sviamento di potere", con la conseguente applicazione dell'ipotesi aggravata prevista dall'art. 615-ter, comma 2, n. 1 (reclusione da 1 a 5 anni). In ogni caso, trattenersi nel sistema

[1] Ha collaborato alla stesura del presente documento Giorgio Valandro Università di Padova

informatico per ragioni diverse dallo svolgimento delle mansioni assegnate è in contrasto con i doveri di lealtà e fedeltà insiti nello statuto del dipendente pubblico e integra il reato base (comma 1).

1. I termini della questione: quando il dipendente si trattiene in violazione dei limiti dell'autorizzazione

Due recenti sentenze della Corte di Cassazione in tema di accesso abusivo a sistema informatico o telematico offrono l'occasione per mettere in evidenza, attraverso il prisma dell'accertamento penale, i confini che non devono essere superati e le responsabilità che gravano sul dipendente pubblico che opera all'interno dei sistemi informatici messi a disposizione dall'amministrazione pubblica.

La norma incriminatrice di riferimento è l'art. 615-ter c.p. (rubricato "Accesso abusivo ad un sistema informatico o telematico"), il quale punisce (con la reclusione fino a 3 anni) chiunque si introduca abusivamente in un "sistema informatico o telematico *protetto da misure di sicurezza*" oppure, in alternativa, "*vi si mantiene*" (ossia lo utilizza) "*contro la volontà espressa o tacita di chi ha il diritto di escluderlo*"[2]. Il c.d. accesso abusivo a sistema informatico, dunque, fa riferimento a due differenti tipologie di condotta:

1) **Introduzione senza autorizzazione.** L'utente accede a un sistema informatico senza avere credenziali autorizzate o i necessari privilegi di accesso;
2) **Permanenza in violazione dei limiti dell'autorizzazione.** L'utente è autorizzato ad accedere al sistema informatico, ma svolge attività che vanno oltre i limiti o per finalità diverse da quelle per le quali è stato autorizzato dal titolare del sistema.

In questo commento non ci si soffermerà sulla prima ipotesi, riferibile all'intrusione in sistemi informatici e banche dati da parte di soggetti non autorizzati, soggetti di norma dotati di elevate conoscenze e capacità tecnico-informatiche (i c.d. hacker) e in ogni caso non autorizzati ad accedere a quel determinato sistema informatico dell'azienda.

Le sentenze in commento, invece, consentono di analizzare l'ipotesi di **violazioni commesse dai dipendenti pubblici** che, essendo **in possesso di credenziali autorizzate** per accedere al sistema informatico della pubblica amministrazione, sono in grado di compiere una serie di atti in genere preclusi alla generalità dei cittadini. Si pone dunque il problema di **individuare i limiti** entro cui il dipendente, autorizzato ad accedervi, può mantenersi e operare (anche per mera consultazione) all'interno dello stesso sistema informatico.

Cassazione penale, sez. V, n. 26530/2021

[2] Art. 615-ter, comma 1: *"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, è punito con la reclusione fino a tre anni."*

Una prima sentenza della Cassazione (Cass., Sez. V Pen., sent. n. 26530 del 12 luglio 2021) tratta del caso di un dipendente dell'INPS condannato per accesso abusivo al "protocollo informatico unificato". Il dipendente, dopo essere stato assegnato a un altro ufficio dello stesso ente, aveva effettuato l'accesso al sistema informatico di servizio al fine di visualizzare una certificazione DURC da lui stesso inserita nel corso dell'attività pregressa svolta nel suo precedente ufficio. Sebbene l'accesso fosse autorizzato a mezzo di credenziali ancora attive, la consultazione dell'area telematica in questione non rientrava più nelle competenze e nei limiti di operatività del dipendente. Per queste ragioni, ossia per la semplice "visualizzazione" di documenti che il dipendente non era (più) autorizzato a gestire, il giudice di primo grado ha condannato il dipendente dell'INPS (con riforma solo parziale in appello), in quanto avrebbe posto in essere un accesso per **ragioni *"ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli era attribuita"***.

Il giudice di legittimità accoglie il ricorso del dipendente dell'INPS, rinviando la sentenza annullata al giudice di merito, in quanto l'accesso era avvenuto per un atto adottato, legittimamente, dallo stesso dipendente che l'aveva inserito nel sistema informatico, mentre la Corte territoriale non avrebbe spiegato perché si tratterebbe di *"un accesso ontologicamente inibito nel caso di specie, nel senso di attività svolta per finalità estranee alle ragioni di istituto e agli scopi sottostanti alla protezione dell'archivio informatico"*[3]. Nel rinnovato esame di merito, "la Corte territoriale dovrà chiarire *in cosa sia consistito lo sviamento di potere, individuando la norma organizzativa asseritamente violata, e spiegare perché verrebbe in rilievo un accesso ontologicamente inibito, in quanto incompatibile con le mansioni del dipendente*" (Cass. n. 26530/2021, pag. 7).

Cassazione penale, sez. V, n. 8911/2021

Una seconda sentenza della Cassazione (Cass., Sez. V Pen., sent. n. 8911 del 4 marzo 2021) riguarda il caso di un militare della Guardia di Finanza condannato in primo grado (con sentenza confermata in appello) per accesso abusivo aggravato alla banca dati SDI (Sistema di indagine del Centro elaborazione dati del Ministero dell'Interno) e rivelazione del segreto d'ufficio, per aver reso informazioni relativamente all'inesistenza di indagini a carico di soggetti terzi.

In questo caso la Suprema Corte rigetta il ricorso dell'imputato, in quanto la sentenza impugnata ha dato ampiamente atto dell'assenza di profili funzionalmente riconducibili a ragioni di ufficio degli accessi allo SDI operati dall'imputato attraverso le proprie credenziali, ragioni che invece devono essere presenti per giustificare l'accesso al sistema informatico da parte del dipendente pubblico. La sentenza di condanna, infatti, dà conto di ben 9 **consultazioni della banca dati non motivate da ragioni d'ufficio**, che dimostrano *"tanto l'ontologica estraneità delle motivazioni della consultazione rispetto alle finalità d'ufficio, che l'abuso della pubblica funzione ricoperta,*

[3] Come osserva la Suprema Corte, inoltre, si è trattato di un unico accesso avvenuto a distanza di sei anni circa dall'adozione dell'atto, in coincidenza temporale con l'instaurazione di un procedimento penale per falso nel quale era stato prodotto proprio quel documento, a firma del ricorrente stesso (Cass. n. 26530/2021, pagg. 6-7).

non solo agevolatrice, ma infungibilmente necessaria per l'acquisizione dei dati" (Cass. pen., V, n. 8911/2021 in commento).

Al di là della specificità della normativa che disciplina il Sistema informatico interforze nell'ambito del Dipartimento della Pubblica Sicurezza oggetto della seconda pronuncia, entrambe le sentenze in commento fanno luce su alcuni aspetti di carattere generale, relativi al non infrequente caso del dipendente pubblico che, abilitato ad accedere alle banche dati istituzionali, acquisisce notizie e dati in **violazione dei doveri insiti nello statuto del dipendente pubblico**, ossia degli obblighi e dei doveri di lealtà e fedeltà che gravano su ogni dipendente pubblico. È necessario verificare, insomma, *"se la condotta addebitata all'imputato rientri o meno nel perimetro dei suoi poteri, in relazione alle funzioni svolte all'interno della struttura cui fa capo il sistema informatico, vale a dire se l'attività posta in essere esuli o meno dalle competenze dell'operatore, ponendosi* ***in contrasto con*** *le prescrizioni relative all'accesso e al trattenimento nel sistema informatico, contenute in* ***disposizioni organizzative impartite dal titolare dello stesso****, indipendentemente dalle finalità soggettivamente perseguite"* (Cass. 26530/2021).

2. La tutela anticipata del c.d. domicilio informatico: (ir-)rilevanza dello scopo perseguito e delle conseguenze della condotta

Senza soffermarsi sulle incertezze teoriche relative alla problematica qualificazione del bene giuridico tutelato (mera estensione del domicilio tradizionale oppure "nuovo" bene giuridico)[4], in questa sede è sufficiente sottolineare come la fattispecie criminosa in esame, secondo l'orientamento giurisprudenziale prevalente, intenda offrire una **tutela anticipata** del c.d. domicilio informatico, inteso non solo come sfera di riservatezza di dati personali, ma più ampiamente come ***jus excludendi alios,*** **a prescindere dalla tipologia dei dati** custoditi dall'utente (persone fisica o giuridica, pubblica o privata), con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali e *lato sensu* aziendali dei dati custoditi e delle relative informazioni (personali o meno)[5].

Quello previsto dall'art. 615-ter c.p. è un **reato di mera condotta**, che si perfeziona con la violazione del c.d. domicilio informatico, senza che sia necessario lo scopo di insidiare la riservatezza degli utenti oppure che si verifichi una effettiva lesione dei

---

[4] L'art. 615-ter è stato collocato tra i delitti contro l'inviolabilità del domicilio, in quanto, secondo il legislatore (legge n. 547/1993), i sistemi informatici rappresenterebbero "un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615" (così la *Relazione* al disegno di legge n. 2773, poi divenuto legge 23 dicembre 1993, n. 547, consultabile in http://legislature.camera.it/_dati/leg11/lavori/stampati/pdf/50216.pdf. Per un primo inquadramento ermeneutico dell'art. 615-ter c.p., vedi: SALVADORI I., *I reati contro la riservatezza informatica*, in CADOPPI A. et al. (a cura di), *Cybercrime*, Torino, UTET, 2019, p. 666 ss.; MELONI M. (a cura di), *Codice penale commentato, art. 615-ter - Accesso abusivo ad un sistema informatico o telematico* [aggiornato da LOMBARDO M.], in *Leggi d'Italia*, Wolters Kluver, www.studiolegale.leggiditalia.it; VERGA G., *Codice penale commentato. Art. 615-ter*, in *De Jure*, Giuffré, www.dejure.it.

[5] Il delitto di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-ter c.p. si configura anche qualora al suo interno non siano memorizzati dati personali, riservati o segreti ovvero non vi sia alcun dato o software, così SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 661.

diritti del titolare del sistema[6]. Si tratta di un reato di **pericolo astratto** (o presunto) perché la soglia di punibilità è arretrata fino a punire il mero ingresso, o mantenimento, nel sistema, a prescindere dalle motivazioni dell'agente o dalle azioni successivamente compiute. La fattispecie è dunque diretta a punire condotte prodromiche alla commissione di più gravi reati informatici (intercettazioni di dati, frodi informatiche, ecc.), i quali, laddove ne siano integrati gli elementi costitutivi, potranno eventualmente concorrere con il delitto di cui all'art. 615-ter.

Per il riconoscimento della responsabilità penale di cui all'art. 615-ter, dunque, **non è necessario che l'autore abbia agito per fini di lucro o per interessi privati**, essendo irrilevante che abbia agito anche **per mera curiosità**. E' sufficiente, infatti, il c.d. dolo generico, ossia la coscienza e volontà di introdursi o di mantenersi nell'altrui sistema informatico o telematico contro la volontà del titolare dello *jus excludendi*: non rileva pertanto lo scopo perseguito da colui che si introduce o si mantiene abusivamente nel sistema.

Del pari irrilevante, ai fini della sussistenza del delitto base, è che l'agente abbia effettivamente carpito informazioni o che abbia danneggiato o impedito il funzionamento del sistema informatico o telematico. Si tratta, in effetti, di eventi che possono integrare un'ipotesi aggravata del delitto in esame (art. 615-ter, comma 2, n. 3) o altre figure di reato che concorrono con l'accesso abusivo (per es. danneggiamento ex art. 635-bis, -ter e -quater).

Come si vede, **trattenersi in un sistema informatico in maniera abusiva configura, *di per sé*, una condotta criminosa**, la quale comporta una responsabilità che, peraltro, risulta aggravata per i dipendenti pubblici (vedi *infra*), i quali devono a maggior ragione essere ben consapevoli dei confini dell'oggetto materiale e della condotta minima che è suscettibile di sanzione (anche) penale, **a prescindere dalle intenzioni e dalle eventuali conseguenze dannose**.

2.1. I confini (molto ampi) della nozione di "sistema informatico o telematico"

La legge n. 547/1993, che ha introdotto nel codice penale i cosiddetti «computer crimes» (tra cui l'art. 615-ter c.p.), non ha enunciato una definizione di «sistema informatico o telematico» oggetto della tutela, dandone per presupposti il significato e i profili tecnici[7]. Il costante sviluppo tecnologico, tuttavia, non consente di individuare con immediatezza il significato dell'espressione "sistema informatico o telematico". D'altra parte, il riferimento a strumenti tecnologici impiegati a fini di automazione è inserito in varie disposizioni di legge, che utilizzano espressioni diverse come

---

6 *"Il delitto di accesso abusivo ad un sistema informatico, che è reato di mera condotta, si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, senza che sia necessario che l'intrusione sia effettuata allo scopo di insidiare la riservatezza dei legittimi utenti e che si verifichi una effettiva lesione alla stessa"*: così Cass. pen., sez. V, 06/02/2006, n. 11689 (rv. 236221).

7 Occorre comunque ricordare che l'art. 1 della Convenzione del Consiglio d'Europa sulla criminalità informatica del 23 novembre 2001 (c.d. Convenzione di Budapest), ratificata dall'Italia con l. n. 48/2008, definisce il "*sistema informatico*" come "*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati*".

“elaboratore elettronico”, “sistema informativo automatizzato”, “centro di elaborazione dati”, ecc.

In assenza di una puntuale classificazione legislativa, è stata la giurisprudenza a fornire una definizione il più ampia possibile, tendenzialmente valida per tutte le fattispecie incriminatrici, che fanno riferimento all'espressione “sistema informatico”. La definizione offerta dalla giurisprudenza è fondata sul passaggio **dal “dato” alla “informazione”**, nel senso che alla funzione di registrazione e di memorizzazione elettronica dei dati come rappresentazione elementare di un fatto, si affianca l'attività complementare di elaborazione e di organizzazione logica, con formazione di un insieme coordinato di informazioni. Un sistema informatico, quindi, si identifica con **un apparato elettronico in grado di elaborare un elevato numero di dati** e capace di produrre come risultato un altro insieme di informazioni, che può essere reso intellegibile da un programma in grado di far cambiare lo stato interno dell'apparato e di variarne, all'occorrenza, il risultato. In questa accezione possono essere ricompresi anche i **sistemi di scrittura o di automazione d'ufficio ad uso individuale** di qualunque tipo e dimensione, oltre che i più complessi sistemi di elaborazione in grado di erogare, anche online, servizi e potenza di calcolo ad una pluralità di utenti interconnessi (cloud services). Quindi anche un normale personal computer può essere considerato un “sistema informatico” in considerazione dell'interconnessione anche potenziale con altri dispositivi elettronici, della pluralità dei software installati, della molteplicità dei dati e delle informazioni trattate e delle funzioni complessivamente svolte.[8]

Con l'espressione **“sistema telematico”**, invece, le disposizioni sui crimini informatici rinviano ad un insieme combinato di apparecchiature idonee alla trasmissione a distanza di dati e di informazioni, attraverso l'impiego di tecnologie dedicate alle telecomunicazioni[9].

Secondo la lettera dell’art. 615-ter, il sistema informatico o telematico deve essere **“protetto da misure di sicurezza”,** senza che tuttavia sia richiesto il loro effettivo aggiramento[10].

Nella nozione “di misure di sicurezza” possono farsi rientrare tutte quelle misure di protezione, al cui superamento è possibile subordinare l'accesso ai dati e ai programmi contenuti nel sistema, analogamente a quanto avviene per i confini che garantiscono la

---

[8] Per evitare vuoti di tutela, la giurisprudenza ha assunto una nozione il più ampia possibile di computer, per ricomprendervi i sistemi a programma variabile, gli elaboratori cosiddetti dedicati, nonché i calcolatori nei quali l'inserimento del software è precostituito mediante «firmware» o circuitazione integralmente prestabilita e non mutabile. A differenza di un mero apparecchio elettronico, inoltre, il sistema informatico è caratterizzato dalla “programmabilità” e dalla variabilità dei risultati. Cfr. MELONI M. (a cura di), *Codice penale commentato*, cit..

[9] Come è noto, il termine “telematica” deriva dalla contrazione semantica dei termini “telecomunicazioni” e “informatica”, al fine di indicare la trasmissione a distanza di informazioni con sistemi di diffusione dei dati.

[10] Come precisa Cass. pen., sez. V, 7.11.2000, n. 12732: *“Non si tratta perciò di un illecito caratterizzato dall’effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio, che è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un "domicilio informatico"*.

delimitazione spaziale del domicilio tradizionale. Per "misure di sicurezza" devono genericamente intendersi tutti quei mezzi di protezione sia logica che fisica[11], complessi o semplici (**anche una singola password**), e a prescindere dal loro livello di efficacia, che il titolare del sistema informatico o telematico ha predisposto al fine di riservare l'accesso o la permanenza alle sole persone da lui autorizzate.

Tuttavia, le misure di sicurezza poste a protezione del sistema non rappresentano un elemento che deve essere necessariamente presente per identificare un sistema informatico (che in astratto potrebbe anche esserne sprovvisto), quanto piuttosto una modalità di **espressione della volontà di impedire l'accesso a persone non autorizzate[12]**. L'art. 615-ter, infatti, punisce, non solo chi si introduce abusivamente (e quindi violando le misure di sicurezza) in un sistema informatico o telematico, ma anche chi, come nelle sentenze in commento, vi si trattiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Senza dilungarsi ulteriormente in questo sforzo definitorio, quello che in questa sede si vuole mettere in evidenza è che gli **ordinari strumenti di elaborazione dati quotidianamente utilizzati dai dipendenti della PA** (banche dati, applicativi gestionali, area intranet, cloud services, ecc.) rientrano nell'ampia nozione di "sistema informatico o telematico" tutelato dall'art. 615-ter c.p. in esame.

Con l'avvertenza che la facilità di accesso alla banca dati, ossia l'assenza o la debolezza delle misure di sicurezza a protezione del sistema, non solleva da responsabilità il dipendente che accede e utilizza la banca dati per ragioni estranee a quelle di servizio (e quindi contro la volontà del titolare del sistema informatico).

Vale la pena di segnalare, infine, la severa aggravante (da 3 a 8 anni di reclusione per il pubblico ufficiale) prevista dello stesso art. 615-ter, terzo comma, qualora i fatti riguardino **sistemi informatici o telematici *"di interesse pubblico"***.

Anche se il contesto normativo può essere ritenuto di carattere speciale (si fa riferimento a sistemi informatici "di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile"), la lettera della norma, che aggiunge la locuzione alternativa *"o comunque di interesse pubblico"*, suggerisce di includere anche **tutte le banche dati delle amministrazioni e delle università pubbliche**.

Ancora una volta, insomma, deve essere colto il monito del legislatore, che richiede ai dipendenti pubblici, e alle relative amministrazioni, la massima attenzione nell'utilizzo dei sistemi informatici o telematici a loro disposizione.

---

[11] Può trattarsi anche di misure di carattere organizzativo, quali ad esempio quelle che disciplinano le modalità di accesso ai locali in cui il sistema è ubicato e indicano le persone abilitate al suo utilizzo (Cass. pen., sez. V, 8.7.2008, n. 37322, rv. 241201).

12 *"La violazione dei dispositivi di protezione non assume rilevanza per sé, ma solo come eventuale manifestazione di una volontà contraria a quella di chi dispone legittimamente del sistema"* (Cass. n. 26530/2021 in commento).

2.2. Eventuali reati successivi alla condotta di accesso abusivo. Le differenze rispetto al reato di rivelazione di segreti d'ufficio

In ragione della particolare struttura del reato in esame (reato di mera condotta), si applicano le sanzioni previste dall'art. 615-ter **anche in assenza di eventuali eventi dannosi successivi** all'intrusione o alla permanenza abusiva all'interno del c.d. domicilio informatico.

Resta fermo, ovviamente, che le conseguenze derivanti dall'accesso abusivo a sistema informatico possono integrare l'ipotesi aggravata di cui all'art. 615-ter, comma 2, n. 3, oppure essere sanzionate in base ad altre figure di reato che concorrono con l'accesso abusivo, come il danneggiamento doloso di dati e sistemi informatici (artt. 635-bis, -ter e -quater)[13], ma anche la rivelazione o utilizzazione di segreti d'ufficio (art. 326 c.p.) oppure l'illecito trattamento di dati personali (art. 167, d.lgs. n. 196/2003, c.d. Codice privacy). Si tratta, come si vede, di fattispecie che possono avere come presupposto un accesso abusivo a sistema informatico o telematico, ma che richiedono ulteriori elementi per il riconoscimento della responsabilità penale rispetto al mero accesso.

- Differenze dall'illecito trattamento dei dati personali

La fattispecie penale dell'illecito trattamento dei dati personali richiede sia un evento dannoso ("nocumento all'interessato") che il dolo specifico ("al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato"), mentre l'accesso abusivo al sistema informatico è punito a prescindere dalle conseguenze dannose realizzate, in quanto si realizza con la sola violazione dello *ius excludendi* del titolare del sistema informatico. Non sussiste pertanto alcun rapporto di specialità tra le due fattispecie, le quali si differenziano per condotte finalistiche e attività materiali[14].

- Differenze dal reato di rivelazione o utilizzazione di segreti d'ufficio

Il reato di rivelazione o utilizzazione di segreti d'ufficio (art. 326 c.p.), oltre ad essere una conseguenza meramente eventuale rispetto all'accesso abusivo al sistema informatico, presuppone la sussistenza di ulteriori elementi che non sono invece richiesti nell'accesso abusivo. Oltre all'abuso della qualifica di pubblico ufficiale (o incaricato di pubblico servizio), per configurare l'ipotesi di cui all'art. 326 è necessario che si tratti di informazioni rilevanti (non futili) e "segrete" (non conosciute), mentre nell'accesso abusivo è **irrilevante la tipologia di dati e di informazioni contenute nel sistema informatico o telematico violato**.

---

[13] Qualora dall'accesso abusivo derivi, quale conseguenza non voluta della condotta, la distruzione o il danneggiamento del sistema nel suo complesso o di singole sue componenti (dati, informazioni o programmi «in esso contenuti») o l'interruzione del funzionamento del sistema, potrà essere integrata la circostanza aggravante prevista nel comma 2, al n. 3. Se la distruzione e il danneggiamento sono invece voluti dall'agente, saranno applicabili le fattispecie di danneggiamento di dati o di sistemi informatici di cui agli artt. 635-bis e 635-quater c.p., in concorso con quella di accesso abusivo ad un sistema informatico (v. SALVADORI I., *I reati contro la riservatezza informatica*, cit., p. 688).

[14] Cass. pen. Sez. V Sent., 05/12/2016, n. 11994 (rv. 269480).

La sentenza n. 8911/2021 in commento fa emergere le diversità tra l'accesso abusivo a sistema informatico, da un lato, e la rivelazione e utilizzazione dei segreti d'ufficio, dall'altro, che corrispondono infatti a due diversi capi di imputazione, trattati rispettivamente nella prima e nella seconda parte della sentenza.

Analogamente a quanto si vedrà per l'ipotesi dell'accesso abusivo aggravato da parte del pubblico ufficiale, anche nella rivelazione dei segreti d'ufficio viene valorizzata la tutela del buon funzionamento e dell'imparzialità della pubblica amministrazione (art. 97 Cost.), che si estrinseca con l'osservanza del segreto d'ufficio inerente al rapporto funzionale tra il pubblico funzionario e l'amministrazione di appartenenza, in tal modo giustificando un ambito del "segreto d'ufficio" non limitato agli "atti segreti". In virtù dell'art. 15 del d.P.R. n. 3/1957 (T. U. degli impiegati civili dello Stato), infatti, la legge non si limita a porre l'obbligo per l'impiegato pubblico di "mantenere il segreto d'ufficio", ma ne definisce anche l'ambito e l'estensione, specificando che l'impiegato *"non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso"*. In questa prospettiva, oggetto materiale del delitto di rivelazione di segreti d'ufficio sono sia le notizie d'ufficio coperte dal segreto, sia quelle indebitamente svelate a chi non è titolare del diritto di accesso agli atti amministrativi o senza il rispetto delle modalità previste, a salvaguardia del bene giuridico del buon andamento e dell'imparzialità della pubblica amministrazione[15].

Come si vede, allora, diversamente da quanto previsto per l'accesso abusivo, il principio di offensività assume un ruolo di limite alla configurabilità del reato di rivelazione di segreto d'ufficio, con riferimento a notizie che siano futili o insignificanti rispetto a principi di buon andamento e imparzialità dell'azione amministrativa. Un limite che, invece, non opera per la configurabilità del reato di accesso abusivo, in quanto **la semplice permanenza** dell'utente all'interno del sistema informatico senza l'autorizzazione o contro la volontà del titolare del sistema **configura, *di per sé*, il reato di cui all'art. 615-ter, a prescindere dalla natura dei dati** contenuti nel sistema informatico, oltre che dalla realizzazione di un qualsivoglia evento dannoso.

3. Violazione delle disposizioni organizzative e operazioni "ontologicamente estranee" alle ragioni di servizio

Le sentenze in commento sottolineano la necessità di verificare se e in che limiti *"il mantenimento nel sistema informatico, anche da parte di chi aveva titolo per accedervi, sia avvenuto in contrasto o meno con la volontà del titolare del sistema stesso, che può manifestarsi, sia in forma esplicita, che tacita"* (Cass. n. 26530/2021).

---

15 Particolare attenzione è dedicata ai dati e alle informazioni presenti all'interno del sistema informatico protetto, accessibili all'utente autorizzato. È espressamente vietata qualsiasi operazione che porti ad una diffusione estranea rispetto alle ragioni di istituto e agli scopi correlati alla protezione dell'archivio informatico. Più precisamente, la disposizione tratta non solo della divulgazione all'esterno di dati o informazioni riservati all'Ente, bensì anche di una visualizzazione o consultazione in generale che sia esorbitante rispetto alle finalità di servizio. Del resto, come osservato nella sentenza in commento (Cass. sentenza n. 8911/2021), "la tutela delle informazioni accessibili ai terzi solo mediante apposito iter procedimentale è valore tanto prioritario da essere tutelato anche laddove l'acquisizione delle notizie sia lecita, assumendo, in tal caso, il fatto rilevanza penale ai sensi deli'art. 12 l. n. 121 del 1981" (nell'ambito dell'ordinamento della pubblica sicurezza).

In particolare, richiamando la consolidata giurisprudenza delle Sezioni unite della Cassazione, si ribadisce che il contrasto con la volontà del titolare del sistema consiste nella:

1) **violazione dei limiti risultanti dal complesso delle prescrizioni impartite dal datore di lavoro**, ossia dalla violazione delle prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole di contratti individuali di lavoro[16];
2) svolgimento di "***operazioni di natura ontologicamente diversa da quelle di cui egli è incaricato*** *ed in relazione alle quali l'accesso era a lui consentito"*[17].

In linea di principio, quindi, il requisito dell'abusività deve essere ancorato a parametri di natura oggettiva (come i limiti posti dal titolare dal sistema e la natura delle operazioni autorizzate), escludendo la rilevanza dei fatti successivi e delle finalità perseguite dall'agente al momento dell'accesso o del mantenimento nel sistema informatico[18].

Tuttavia, con riferimento ai **dipendenti pubblici**, le Sezioni Unite della Cassazione, non esenti da critiche da parte della dottrina[19], hanno già avuto modo di dirimere i contrasti giurisprudenziali sorti sulla portata dell'espressione **"operazioni ontologicamente estranee" a quelle consentite**, nell'ipotesi di un pubblico ufficiale o un incaricato di pubblico servizio che, "*formalmente autorizzato all'accesso ad un sistema informatico o telematico, ponga in essere una condotta che concreti uno sviamento di potere, in quanto mirante al raggiungimento di un fine non istituzionale,* ***pur in assenza di violazione di specifiche disposizioni regolamentari ed organizzative****"* (Cass. pen. SS.UU. del 18/05/2017, n. 41210, c.d. "Savarese").

Si tratta, come si vede, di una interpretazione che estende ulteriormente il campo di applicazione della norma incriminatrice, in quanto attribuisce rilevanza non solo agli elementi oggettivi della violazione delle prescrizioni formalmente poste dal titolare del sistema o della oggettiva natura delle operazioni realizzate, ma anche a un elemento di natura soggettiva come le finalità perseguite[20].

---

16 Vedi Cass., SS.UU., n. 4694 del 27/10/2011 (c.d. sentenza "Casani"): *"integra il delitto previsto dall'art. 615-ter cod. pen. colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso, rimanendo invece irrilevanti, ai fini della sussistenza del reato, gli scopi e le finalità che abbiano soggettivamente motivato l'ingresso nel sistema".*

17 Cass., SS.UU., n. 4694/2011 ("Casani").

18 Cfr. BERTOLESI R., *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere*, in *Diritto penale contemporaneo*, 10/2017, pp. 283 ss., consultabile in https://archiviodpc.dirittopenaleuomo.org/d/5634-accesso-abusivo-a-un-sistema-informatico-e-reato-la-condotta-del-pubblico-ufficiale-commessa-con-cd.

19 Vedi, tra gli altri, SALVADORI, *op. cit.*, 684

20 Si osserva criticamente (SALVADORI, *op. cit.*, 683) che la determinazione dell'«abuso di poteri» o della «violazione dei doveri» da parte del pubblico ufficiale andrebbe ricostruita, per evitare che la condotta di accesso "a forma vincolata" venga fatta coincidere con il mero eccesso o sviamento di poteri, sulla base di un parametro oggettivo o normativo (extrapenale), da individuarsi nell'insieme delle leggi, dei regolamenti che determinano i poteri, i doveri o le competenze inerenti alla funzione ed al servizio pubblico, ovvero delle "regole" di condotta, anche di carattere non strettamente tecnico, che disciplinano l'accesso del funzionario pubblico al sistema informatico della pubblica amministrazione al quale è addetto.

La severità della responsabilità che grava sul dipendente pubblico merita un opportuno chiarimento, anche al fine di orientare i comportamenti dei dipendenti e delle stesse amministrazioni pubbliche "titolari del sistema".

3.1. L'aggravante dell'abuso dei pubblici poteri

Il reato di accesso abusivo è un reato c.d. comune, in quanto può essere commesso da "chiunque", sia che si tratti di un soggetto interno (dipendente o collaboratore) sia che si tratti un soggetto esterno rispetto al titolare del sistema. Tuttavia, la qualifica di **"pubblico ufficiale" o di "incaricato di pubblico servizio"**, non necessaria per la configurazione del reato di accesso abusivo, è prevista come aggravante (da 1 a 5 anni di reclusione) esclusivamente soggettiva, se il fatto è commesso "con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio" (art. 615-ter, secondo comma, n. 1).

La mera qualifica di pubblico ufficiale (o di "incaricato di pubblico servizio"), quindi, non è in astratto sufficiente a configurare l'aggravante in esame, essendo necessario che il fatto sia commesso dall'operatore **con abuso dei poteri o in violazione dei doveri inerenti alla sua funzione**, di modo che la qualità soggettiva dell'agente abbia quantomeno agevolato la realizzazione del reato. In altri termini, *"né la qualità rivestita dal soggetto agente, né l'abuso di tale qualità fondano ex se il profilo aggravatore del fatto tipico, che invece si giustifica in presenza di un abuso potere in quanto teleologicamente orientato a scopi diversi da quelli collegati alle attribuzioni pubbliche"* (così Cass. n. 8911/2021)[21].

Tuttavia, come evidenziato nella sentenza n. 26530/2021 in commento, **per i pubblici ufficiali o gli incaricati di pubblico servizio *"il reato è sempre aggravato***, *proprio perché la circostanza è inscindibilmente collegata a quella qualità soggettiva ed in tutti i casi la configurata aggravante comporta un abuso, che ben può connotarsi delle caratteristiche dell'esecuzione di "operazioni ontologicamente estranee" rispetto a quelle consentite. Invero la norma si riferisce a soggetti che accedono al sistema e vi si trattengono abusando della propria qualità soggettiva, che rende più agevole la realizzazione della condotta tipica, oppure che connota l'accesso in sé quale comportamento di speciale gravità"* (Cass. pen. SS.UU. del 18/05/2017, n. 41210, c.d. "Savarese").

In effetti, la condotta del pubblico ufficiale (o incaricato di pubblico servizio) che accede o si trattiene nel sistema informatico per **scopi diversi da quelli istituzionali** deve considerarsi "abusiva" in base ai principi generali che governano l'azione amministrativa, la quale deve essere orientata esclusivamente al perseguimento dei fini determinati dalla legge, secondo i generali principi di buon andamento e imparzialità (art. 1, legge n. 241/1990; art. 97 Cost.).

---

[21] Per queste ragioni, la sentenza della Cassazione in commento respinge il ricorso, in quanto la sentenza di condanna impugnata ha dato ampiamente atto dell'assenza, negli accessi al sistema informatico operati dall'imputato attraverso le proprie credenziali, di profili funzionalmente riconducibili a ragioni di ufficio, in questo modo *"giustificando tanto l'ontologica estraneità delle motivazioni della consultazione rispetto alle finalità d'ufficio, che l'abuso della pubblica funzione ricoperta, non solo agevolatrice, ma infungibilmente necessaria per l'acquisizione dei dati"* (Cass. n. 8911/2021 in commento).

3.2. Sviamento di potere e rispetto dei doveri d'ufficio

Secondo l'orientamento ormai consolidato della Cassazione, quindi, il trattenimento o l'utilizzo del sistema informatico dell'ufficio a cui è addetto il pubblico ufficiale o l'incaricato di pubblico servizio deve considerarsi abusivo, anche se avvenuto utilizzando credenziali autorizzate e anche in assenza di ulteriori espressi divieti di accesso, quando è connotato dall'**abuso delle proprie funzioni** da parte dell'agente, ossia da un c.d. **sviamento di potere**, inteso come "*un uso del potere in* ***violazione dei doveri di fedeltà*** *che ne devono indirizzare l'azione nell'assolvimento degli specifici compiti di natura pubblicistica a lui demandati*" (Cass. SS.UU., n. 41210/2021, *Savarese*, cit.).

Il c.d. sviamento di potere è una delle tipiche manifestazioni della più generale categoria amministrativistica del vizio di "eccesso di potere" e ricorre quando l'atto amministrativo non persegue un interesse pubblico, ma un interesse privato, ossia quando il funzionario pubblico nella sua attività concreta persegue una finalità diversa da quella che gli assegna in astratto la **legge sul procedimento amministrativo** (art. 1, legge n. 241 del 1990). Gli stessi principi di buon andamento e imparzialità sanciti dalla legge sul procedimento amministrativo hanno trovato progressiva attuazione anche nelle disposizioni in tema di **organizzazione del pubblico impiego,** fra le quali assumono speciale rilievo le disposizioni che disciplinano lo *status* della persona dotata di funzioni pubbliche, dal c.d. Testo Unico sul pubblico impiego (d.lgs. 165/2001) al Codice di comportamento dei pubblici dipendenti, e più in generale gli articoli 54, 97 e 98 della Costituzione, che richiedono al dipendente pubblico l'adesione a "principi di etica pubblica": i pubblici ufficiali e gli incaricati di pubblico servizio sono tenuti ad agire per il perseguimento delle finalità istituzionali in vista delle quali il rapporto funzionale è instaurato.

Lo sviamento di potere viene così ricondotto all'interno delle nozioni di abusività della condotta e del fatto commesso in violazione dei doveri di ufficio[22]. Il trattenimento o l'utilizzo di un sistema informatico per ragioni estranee a quelle di ufficio si traduce per il dipendente pubblico in una condotta abusiva, ponendosi in un rapporto di **"ontologica incompatibilità" con la funzione pubblica** svolta[23].

---

[22] Ciò emerge con particolare evidenza nella giurisprudenza sul reato di abuso di ufficio: *"ai fini della configurabilità del reato di abuso d'ufficio, sussiste il requisito della violazione di legge non solo quando la condotta del pubblico ufficiale sia svolta in contrasto con le norme che regolano l'esercizio del potere, ma anche quando la stessa risulti orientata alla sola realizzazione di un interesse collidente con quello per il quale il potere è attribuito, realizzandosi in tale ipotesi il vizio dello sviamento di potere, che integra la violazione di legge poiché lo stesso non viene esercitato secondo lo schema normativo che ne legittima l'attribuzione"* (Cass. SS.UU., *Savarese*, cit.). La rilevanza penale del c.d. sviamento di potere è stata peraltro ribadita recentemente dalla giurisprudenza anche a seguito della riforma dell'art. 323 c.p. (Cass. pen. Sez. VI Sent., 09/12/2020, n. 442, rv. 280296-01).

[23] Si segnalano, ancora una volta, le considerazioni critiche di SALVADORI, op. cit., 684, secondo il quale "il carattere «abusivo» dell'accesso ad un sistema informatico da parte di un funzionario pubblico non può essere determinato sulla base dei principi generali (trasparenza, pubblicità, probità, fedeltà, ecc.) che conformano lo statuto della pubblica amministrazione. Se si accettasse tale interpretazione, si finirebbe con il riconoscere all'autorità giudiziaria un ampio potere discrezionale. Anche le condotte di introduzione o di mantenimento in un sistema informatico realizzate da un pubblico ufficiale legittimato ad accedervi, ma prive di utilità o di convenienza per la pubblica amministrazione potrebbero essere considerate come un «eccesso di potere» e, di conseguenza, ritenute penalmente rilevanti". Una ricostruzione giudiziale ex post, sulla base di una valutazione discrezionale relativa alla compatibilità o «ontologica contrarietà» delle operazioni realizzate dal funzionario pubblico, per cui "il soggetto attivo non sempre avrebbe la consapevolezza di accedere al sistema informatico «abusivamente»".

Se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, si realizza un vero e proprio **"sviamento di potere"**, con conseguente applicazione della circostanza aggravante (reclusione da 1 a 5 anni) prevista dall'art. 615-ter, comma 2, n. 1[24]. Il più rigoroso trattamento sanzionatorio e la procedibilità di ufficio prevista per l'aggravante di cui all'art. 615-ter, comma 2, n. 1, si giustifica in quanto si tratta di un abuso qualificato dall'essere commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, ossia da soggetti dotati di poteri disciplinati da norme di diritto pubblico e da atti autoritativi[25].

Diversamente, il **dipendente pubblico addetto a "semplici mansioni d'ordine"** e ad attività "meramente materiali", che violi le disposizioni del titolare del sistema accedendo al di fuori delle sue mansioni, non commette il reato aggravato in esame, ma risponde per il reato "base" di cui all'art. 615-ter c.p., comma 1, a prescindere dalle finalità perseguite.

In ogni caso, quindi, a parte la difficoltà di delimitare la nozione di dipendente pubblico da quella di incaricato di pubblico servizio (entrambe caratterizzate dall'assenza di poteri autoritativi o certificativi)[26], il trattenimento e l'utilizzo del sistema informatico da parte del dipendente pubblico per scopi diversi da quelli istituzionali assume rilevanza penale ai sensi dell'art. 615-ter, anche in assenza della formale violazione di specifiche prescrizioni provenienti dal titolare del sistema: *"è penalmente rilevante anche la condotta del soggetto che, pur essendo abilitato ad accedere al sistema informatico o telematico, vi si introduca con la password di servizio per raccogliere dati protetti per finalità estranee alle ragioni di istituto ed agli scopi sottostanti alla protezione dell'archivio informatico, utilizzando sostanzialmente il sistema per finalità diverse da quelle consentite"* (Cass. pen., sez. V, n. 8911/2021 in commento).

---

24 *"Integra il delitto previsto dall'art. 615-ter c.p., comma 2, n. 1, 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"* (Cass. SS.UU., *Savarese*, cit.).

25 Le definizioni di "pubblico ufficiale" e di incaricato di pubblico servizio" agli effetti della legge penale sono contenute, rispettivamente, negli artt. 357 e 358 del c.p. In entrambi i casi, si tratta di attività disciplinate da norme di diritto pubblico e da atti autoritativi (c.d. limite esterno). Tuttavia, il pubblico servizio si connota, rispetto alla pubblica funzione, per la mancanza dei poteri tipici di quest'ultima: l'incaricato di pubblico servizio, cioè, non partecipa alla formazione della volontà dell'ente, né alla sua manifestazione e non ha poteri autoritativi, né certificativi (c.d. limite interno). In ogni caso potrà indifferentemente trattarsi di agenti facenti capo ad enti pubblici o di privati, poiché ciò che rileva è unicamente il criterio di disciplina. Inoltre, la qualifica di incaricato di pubblico servizio viene meno rispetto a coloro che svolgono "semplici mansioni d'ordine" o "prestano opera meramente materiale", trattandosi di mansioni che nulla hanno di pubblicisticamente rilevante (si pensi ad es. agli addetti alle pulizie di un ente pubblico). Si tratta comunque di definizioni controverse, sulle quale non mancano i contrasti giurisprudenziali. Sul punto si rinvia a STORTONI L., *Delitti contro la pubblica amministrazione*, in AA.VV., *Diritto penale: Lineamenti di parte speciale*, Bologna, Monduzzi, 2016, p. 111 ss.

26 Cfr. SEMINARA, Sub *Art. 358,* in FORTI G. - SEMINARA S. - ZUCCALA' G., *Commentario breve al codice penale* Padova, CEDAM, 2017 p. 1169, che denuncia "l'usura del tempo" della nozione di "pubblico impiegato", anche alla luce della privatizzazione del lavoro pubblico. D'altra parte, l'ipotesi di un dipendente pubblico che, autorizzato ad accedere a un sistema informatico o telematico, sia chiamato a svolgere attività "meramente materiale" è più di portata astratta che concreta, come emerge dalla casistica giurisprudenziale relativa all'applicazione dell'art. 358 c.p. (sono stati trattati alla stregua di "incaricati di pubblico servizio", tra gli altri: il collaboratore scolastico rispetto alle funzioni di vigilanza e sorveglianza degli studenti, le funzioni di custode, di addetto ai rapporti con il pubblico, di cassiere).

4. Conclusioni riassuntive (e organizzative)

Il dipendente pubblico che, pur essendo formalmente autorizzato ad accedere con specifiche credenziali (username e password) a un determinato sistema informatico o telematico dell'amministrazione (per es. una banca dati gestionale), si trattiene nel sistema "*contro la volontà espressa o tacita di chi ha il diritto di escluderlo*", commette il reato di cui all'art. 615-ter (Accesso abusivo a sistema informatico o telematico).

Quello previsto dall'art. 615-ter c.p. è un reato che si perfeziona con la sola violazione del c.d. domicilio informatico, senza che sia necessario che si verifichi una effettiva lesione dei diritti del titolare del sistema e a prescindere dalle motivazioni dell'agente, dalla natura dei dati contenuti nel sistema informatico o dalle eventuali azioni successivamente compiute.

Il **contrasto con la volontà del titolare del sistema** può derivare, alternativamente, da:

1) violazione dei limiti risultanti dal complesso delle **prescrizioni impartite dal datore di lavoro** (disposizioni organizzative interne, prassi aziendali o clausole di contratti individuali di lavoro);
2) svolgimento di attività ontologicamente estranee alle **ragioni di servizio** (sviamento di potere).

Misure tecniche e organizzative

È necessario, quindi, che l'Amministrazione, in qualità di titolare del sistema, definisca l'organizzazione, le mansioni e le istruzioni da impartire agli operatori autorizzati, adottando tutte le **misure tecniche e organizzative** per garantire la sicurezza, oltre che la riservatezza, dei sistemi informatici o telematici messi a disposizioni del personale per lo svolgimento delle relative mansioni. Il dipendente pubblico, infatti, deve essere messo nelle condizioni di poter conoscere con precisione sia **i confini delle proprie mansioni all'interno dell'organizzazione**, sia le modalità di accesso, consultazione e utilizzo dei sistemi informatici o telematici che è chiamato a utilizzare quotidianamente.

L'Amministrazione, inoltre, deve effettuare un'attenta valutazione delle mansioni affidate ai propri operatori, fornendo soltanto gli accessi necessari per lo svolgimento delle relative attività. A tal fine, l'organizzazione deve prevedere, e **documentare**, quantomeno:

a) le reti, i servizi di rete e le banche dati ai quali i singoli utenti o gruppi di utenti devono accedere per le loro attività;
b) una procedura per la gestione dei diritti di accesso privilegiati;
c) la rimozione o adattamento dei diritti di accesso non solo quando viene meno il rapporto di lavoro con il dipendente, ma anche quando sono modificate le modalità di esecuzione del rapporto di lavoro (sede di servizio, ufficio o mansioni nuovi);

d) una formazione degli operatori differenziata in base alle mansioni svolte, con specifico riferimento all'utilizzo e alla sicurezza dei sistemi informatici e alla protezione dei dati personali;
e) una procedura che preveda il periodico riesame dei privilegi di accesso degli operatori.

La responsabilità del dipendente pubblico

In ogni caso, il dipendente pubblico può trattenersi e utilizzare i sistemi informatici aziendali **esclusivamente per svolgere le mansioni assegnate,** nel rispetto dei principi di buon andamento e imparzialità dell'agire amministrativo. Non costituiscono una scusante le eventuali carenze dell'Amministrazione nella determinazione delle misure tecniche e organizzative, come può avvenire nel caso di autorizzazioni rilasciate ad ampie categorie di utenti interni (raggruppati per area, anziché per mansioni) oppure in occasione del cambio di collocazione del personale dipendente o di variazione della qualifica interna originariamente attribuita.

Nel caso del pubblico ufficiale o di incaricato di pubblico, lo svolgimento di operazioni estranee alle ragioni d'ufficio realizza, anche alla luce della giurisprudenza più recente, un vero e proprio "sviamento di potere", con la conseguente applicazione dell'ipotesi aggravata prevista dall'art. 615-ter, comma 2, n. 1 (reclusione da 1 a 5 anni).

In ogni caso, è in contrasto con i **doveri di lealtà e fedeltà insiti nello statuto del dipendente pubblico**, trattenersi e utilizzare il sistema informatico, anche se con credenziali autorizzate e formalmente senza violare le istruzioni impartite dall'amministrazione di appartenenza, per ragioni ontologicamente estranee a quelle di servizio, ossia al di fuori delle funzioni assegnate all'interno dell'organizzazione, a prescindere dalle finalità perseguite (fosse anche solo mera curiosità).