

**Penale Sent. Sez. 5 Num. 26530 Anno 2021**

**Presidente: SABEONE GERARDO**

**Relatore: BELMONTE MARIA TERESA**

**Data Udiienza: 17/05/2021**

**SENTENZA**

sul ricorso proposto da

██████████ nato a ██████████ il ██████████

Avverso la SENTENZA del 13/01/2020 della CORTE di APPELLO di LECCE

visti gli atti, il provvedimento impugnato e il ricorso;

udita la relazione svolta dal consigliere MARIA TERESA BELMONTE;

letta la requisitoria scritta, del 28 aprile 2021, del Sostituto Procuratore Generale, Lucia ODELLO, che ha concluso per l'inammissibilità del ricorso, a cui si è riportata in udienza.

letta la memoria del 28 aprile 2021 dell'avvocato Edoardo URSO, difensore e procuratore speciale della parte civile INPS, che ha depositato memoria scritta e nota spese, e concluso per l'infondatezza del ricorso.

sentito l'avvocato Ferruccio Gianluca PALAZZO, difensore del ricorrente, che ha depositato certificazione della Corte di appello di Lecce, dalla quale risulta che avverso la sentenza n. 1222/2016, nel giudizio promosso da ██████████ contro l'INPS, non risulta proposto ricorso ai sensi dell'art. 347 cod. proc. civ., né l'istanza di revocazione per i motivi di cui ai nn. 4 e 5 dell'art. 395 stesso codice. L'avvocato Palazzo insiste per l'accoglimento del ricorso.

Dato atto che con provvedimento del 14 aprile 2021 è stata disposta la trattazione nelle forme orali ordinarie della causa, su richiesta del difensore del ricorrente.

Corte di Cassazione - copia non ufficiale

## RITENUTO IN FATTO

1. Con la sentenza impugnata, la Corte di appello di Lecce ha parzialmente riformato, solo con riguardo al trattamento sanzionatorio, la decisione del Tribunale di Brindisi - che aveva dichiarato [redacted] colpevole di accesso abusivo al "protocollo informatico unificato" dell'I.N.P.S. - sede di Brindisi, di cui è dipendente.

1.1. Secondo la ricostruzione dei giudici di merito, il ricorrente, precedentemente assegnato all'Ufficio competente per il rilascio dei DURC aziendali, dopo essere stato trasferito ad altra unità organizzativa, aveva fatto accesso, con le proprie credenziali, all'altra sezione ( BURC) del predetto sistema informatico, in particolare visionando una certificazione, a suo tempo, da lui stesso inserita; in tal modo, avrebbe posto in essere un accesso per ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso gli era attribuita.

2. Propone ricorso per cassazione l'imputato, con il ministero del difensore di fiducia, che svolge due motivi.

2.1. Con il primo, denuncia violazione di norme processuali ( art. 181 co. 4 cod. proc. pen.) e vizio della motivazione, perché mancante, lamentando violazione del diritto di difesa per compressione del diritto alla prova dell'imputato. Infatti, il giudice di merito aveva escusso i testi della difesa con le garanzie previste dall'art. 210 cod. proc. pen., cosicché essi si avvalevano della facoltà di non rispondere, mentre non essendo in alcun modo coinvolti nel processo, essi avrebbero dovuto essere sentiti quali testimoni, nelle forme ordinarie.

2.2. Con il secondo motivo vengono denunciati violazione di legge penale e correlato vizio della motivazione con riguardo alla configurabilità del reato di accesso abusivo, che la Corte di appello ha ravvisato senza dar conto delle ragioni ontologicamente estranee rispetto a quelle per le quali la facoltà di accesso al sistema informatico gli era attribuita. Sostiene la Difesa che il reato in questione sia configurabile solo laddove l'accesso a un archivio informatico protetto non possa essere autorizzato gerarchicamente, poiché esporrebbe il titolare del sistema al rischio di un danno connesso a un accesso operato in contrasto con le regole fissate. Si segnala, invece, come il giudice civile, nel decidere la controversia di lavoro relativa alla sanzione disciplinare inflitta al ricorrente dall'ente datoriale, abbia affermato che l'accesso avrebbe dovuto essere autorizzato dai superiori. Il diverso approdo interpretativo risente, secondo la Difesa, dell'assenza di riferimenti certi volti a denotare il confine delle ragioni ontologicamente estranee. Certo è che, in sede civile, per il medesimo fatto, è stata irrogata una sanzione disciplinare minima ( rimprovero scritto), poi annullata dalla Corte di appello, che aveva accertato la regolarità della condotta amministrativa del ricorrente. Si duole la Difesa che la Corte penale non abbia specificato se l'accesso in questione fosse assentibile dal superiore gerarchico preposto, con corrispondente facoltà del soggetto che opera di potere farne richiesta; in tal modo, non è stata fatta corretta applicazione del principio di diritto affermato dalle Sezioni Unite Savarese, avendo i giudici di merito ommesso di valutare oggettivamente il finalismo materiale della condotta, ovvero senza affrontare il tema della esistenza o meno di una giustificazione

causale in una logica di relazione con il lavoro svolto, atteso che l'atto a cui il ricorrente ha avuto accesso era stato da lui stesso adottato e inserito nel sistema sei anni prima, mentre l'accesso incriminato era stato indotto dall'aver appreso che, per quella certificazione, era in corso un procedimento per falso.

### CONSIDERATO IN DIRITTO

Il ricorso è fondato, per quanto si dirà, e la sentenza impugnata deve essere annullata con rinvio al giudice di merito per nuovo giudizio.

1. Non è fondato il primo motivo, dal momento che, invece, correttamente, il giudice di merito ha escusso i testimoni con le modalità di cui all'art. 210 cod. proc. pen., onde evitare di incorrere nella possibile sanzione della inutilizzabilità delle dichiarazioni, prevista dall'art. 63, comma 2, cod. proc. pen.. Né, all'evidenza, può fondatamente sostenersi che le aspettative, meramente eventuali, del ricorrente a sentire potenzialmente dichiarazioni a sé favorevoli possano prevalere sulla garanzia prevista per il dichiarante, che si trovi nella condizione processuale di potere divenire assumere la veste di indagato o imputato di reato connesso o di reato collegato a norma dell'art. 371, comma 2, lett. b), cod. proc. pen..

2. E' fondato, invece, il secondo motivo.

Grazie all'intervento delle Sezioni Unite, si è chiarito, con due distinte pronunce, che «*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*» (Sez. U, n. 4694 del 27/10/2011, dep. 2012, Casani, Rv 251269). Il principio ha ricevuto una integrazione dalla successiva sentenza "Savarese" che, pronunciandosi sull'ipotesi aggravata prevista dal secondo comma della disposizione in esame, in relazione al fatto commesso da un funzionario di cancelleria, il quale, sebbene legittimato ad accedere al Registro informatizzato delle notizie di reato - c.d. Re.Ge. - conformemente alle disposizioni organizzative della Procura della Repubblica presso cui prestava servizio, aveva preso visione dei dati relativi ad un procedimento penale per ragioni estranee allo svolgimento delle proprie funzioni, ha ritenuto che, in tal modo, fosse stata realizzata un'ipotesi di sviamento di potere, ed ha affermato che il delitto previsto dall'art. 615-ter cod. pen. risulta configurato dalla condotta di «*colui il quale, 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 rispetto a quelle per le quali la facoltà di accesso gli è attribuita*» (così, Sez. U, n. 41210 del 18/05/2017, Savarese, Rv. 271061).

2.1. Alla luce di un orientamento che ormai può definirsi in termini di "diritto vivente", integra, quindi, la fattispecie criminosa di accesso abusivo ad un sistema informatico o telematico protetto, prevista dall'art. 615 ter c.p., 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, ovvero ponga in essere operazioni di natura ontologicamente diversa da quelle per le quali l'accesso è consentito. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema (Sez. un., 27/10/2011, n. 4694; Cass., Sez. V, 26/06/2015, n. 44403, rv. 266088; Sez. V, 15/01/2015, n. 15950; Sez. V, 20/06/2014, n. 44390, rv. 260763; Sez. V, 30/09/2014, n. 47105).

2.2. In punto di diritto, si deve, altresì, premettere, perché qui rileva, che, ai fini della configurabilità del reato di accesso abusivo ad un sistema informatico, nel caso di soggetto dotato delle credenziali per accedere ad una banca dati riservata ( come nel caso di specie), è necessario accertare il superamento, su un piano oggettivo, dei limiti e, pertanto, la violazione delle prescrizioni relative all'accesso ed al trattenimento nel sistema informatico, contenute in disposizioni organizzative impartite dal titolare dello stesso. Occorre verificare, cioè, 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 (Sez. 5, n. 15054 del 22/02/2012, Rv. 252479; Sez. 5, n. 10083 del 31/10/2014 (dep. /2015) Rv. 263454). Nella ricostruzione della fattispecie sottoposta al suo esame, dunque, il giudice di merito deve porsi nella prospettiva di verificare se l'introduzione o 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 (sez. V, 10.12.2009, n. 2987, rv. 245842), dal momento che nel delitto di accesso abusivo ad un sistema informatico o telematico, 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 (Sez. 5, n. 2987 del 10/12/2009 (dep. 2010 ) Rv. 245842; Sez. 5, n. 12732 del 07/11/2000, Rv. 217743 ).

2.3. Le Sezioni Unite, invero, già con la sentenza Casani hanno optato per l'interpretazione più estensiva già oggetto di numerose pronunce, secondo la quale 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. L'autorevole precedente è giunto a questa conclusione considerando che la norma in esame punisce non soltanto l'abusiva introduzione nel sistema (da escludersi nel caso di possesso del titolo di legittimazione), ma anche l'abusiva permanenza in esso contro la volontà di chi ha il diritto di escluderla e che, 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. La successiva sentenza delle Sezioni Unite " Savarese", ha precisato, rispetto ad alcune incertezze interpretative, la direzione esegetica di Sezioni Unite "Casani" quanto, in particolare, alla rilevanza o meno della violazione di norme specifiche che disciplinassero l'accesso al sistema. Più precisamente, con la sentenza "Savarese", è stato approfondito e specificato il concetto di "operazioni ontologicamente estranee" a quelle consentite, qualora la condotta criminosa sia posta in essere da un pubblico ufficiale o da un incaricato di pubblico servizio, evocando sia l'art. 1 della I. 241 del 1990 che gli artt. 54, 97 e 98 della Costituzione, ponendosi nel solco di Sezioni Unite Casani, da cui era già evincibile come fosse sufficiente, per integrare la fattispecie penale, che il soggetto avesse travalicato i limiti propri dell'autorizzazione che gli era stata concessa (il soggetto agente — così Sezioni Unite Casani — è penalmente responsabile «*sia allorquando violi i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema [...] 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*»), nonché nella scia di un corposo filone giurisprudenziale che aveva preceduto anche Sezioni Unite Casani (come ricostruito da Sez. 5 n. 47510 del 09/07/2018, Rv. 274406).

2.4. Come hanno chiarito sia le Sezioni Unite <sup>Casani</sup>~~Savani~~ che "Savarese" - quest'ultima avendola peraltro espressamente qualificata - «*quella prevista dal secondo comma, n. 1, della norma incriminatrice è qualificabile come circostanza aggravante esclusivamente soggettiva, nel senso che descrive la condotta punibile in quanto posta in essere da determinati soggetti. Il pubblico ufficiale, l'incaricato di pubblico servizio, l'investigatore privato e l'operatore del sistema possono rispondere del reato solo in forza della previsione del secondo comma. Per tali soggetti 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*» ( Sez. Un. Savarese, in motivazione; conf. (Sez. 5, n. 25944 del 09/07/2020, Rv. 279496).

2.5. Nel dirimere, quindi, il contrasto circa la possibilità di ravvisare l'abusività dell'accesso nella violazione dei principi che presiedono allo svolgimento dell'attività amministrativa, quali sinteticamente enunciate dall'art. 1 legge 7 agosto 1990, n. 241, Sezioni Unite Savarese hanno affrontato il non infrequente caso del soggetto, in specie pubblico ufficiale o equiparato, che, abilitato e senza precisazione di limiti espressi alle possibilità di accesso e trattenimento nel sistema pubblico, acquisisca da questo notizie e dati, in violazione dei doveri insiti nello statuto del pubblico dipendente, nel complesso degli obblighi e dei doveri di lealtà a lui incombenti. Hanno così affermato che non esce dall'area di applicazione della norma la situazione nella quale l'accesso o il mantenimento nel sistema informatico dell'ufficio a cui è addetto il pubblico ufficiale

o l'incaricato di pubblico servizio, seppur avvenuto a seguito di utilizzo di credenziali proprie dell'agente ed in assenza di ulteriori espressi divieti in ordine all'accesso ai dati, si connoti, tuttavia, dall'abuso delle proprie funzioni da parte dell'agente, rappresenti cioè uno sviamento di potere, 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. La sentenza ha condiviso, con autorevole dottrina, l'affermazione che «sotto lo schema dell'eccesso di potere si raggruppano tutte le violazioni di quei limiti interni alla discrezionalità amministrativa, che, pur non essendo consacrati in norme positive, sono inerenti alla natura stessa del potere esercitato». Lo sviamento di potere è una delle tipiche manifestazioni di un tale vizio dell'azione amministrativa e ricorre quando l'atto non persegue un interesse pubblico, ma un interesse diverso (di un privato, del funzionario responsabile, ecc.). Si ha quindi "sviamento di potere" quando nella sua attività concreta il pubblico funzionario persegue una finalità diversa da quella che gli assegna in astratto la legge sul procedimento amministrativo (art. 1, legge n. 241 del 1990). In tal senso, il Massimo consesso di legittimità ha privilegiato l'interpretazione che aveva evidenziato il principio di cui all'art. 1 della legge n. 241 del 1990, in base al quale «l'attività amministrativa persegue fini determinati dalla legge ed è retta da criteri di economicità, efficacia, imparzialità, pubblicità, trasparenza, secondo le modalità previste dalla presente legge e dalle disposizioni che disciplinano singoli procedimenti, nonché dai principi dell'ordinamento comunitario». (...) Si è ritenuto (Sez. U, n. 155 del 29/09/2011, Rossi, dep. 2012, Rv. 251498) che «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» ( Sez. Un. Savarese, cit.).

2.6. Orbene, osserva il Collegio che questa non è stata la prospettiva in cui si sono collocati i giudici di merito nel valutare il peculiare caso in esame, in cui - a differenza di quelli esaminati nella giurisprudenza di questa Corte ( cfr. *ex plurimis*, Sez. 5 - , n. 37339 del 15/07/2019, Rv. 277535, Sez. 5, n. 25944 del 09/07/2020, Rv. 279496, Sez. 5, n. 18284 del 25/03/2019, Rv. 275914 - Sez. 5 n. 565 del 29/11/2018 (dep. 2019 ) Rv. 274392), tutti riguardanti ipotesi di accessi finalizzati a carpire informazioni riservata o che essi, comunque, non erano legittimati a conoscere, compresi quelli scrutinati dalle Sezioni Unite, sopra richiamate - l'accesso è avvenuto per un atto adottato, legittimamente, dallo stesso dipendente, che l'aveva inserito nel sistema informatico; non viene, quindi, in rilievo un accesso ad atti riservati, rispetto ai quali, cioè, il dipendente dovesse essere ritenuto estraneo. Né va trascurata la circostanza che l'accesso ( unico) è 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. Detta circostanza non è priva di ricadute al momento della

individuazione dell'interesse oggettivamente perseguito con detta attività, rilevando ai fini della configurabilità della fattispecie dello sviamento di potere. Trattandosi, all'evidenza, di un accesso non finalizzato, come normalmente avviene, ad acquisire conoscenza di atti di altro ufficio, o di informazioni riservate, la Corte avrebbe dovuto chiarire 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.

Dovrà chiarire la Corte di merito perché il ricorrente avrebbe utilizzato il sistema per finalità diverse da quelle consentite, violandolo; perché la condotta sarebbe stata orientata alla realizzazione di un interesse collidente con quello per il quale il potere è attribuito, altresì, prendendo posizione in ordine alla affermazione, contenuta nella sentenza della stessa Corte - sezione civile /lavoro n. 1088/2019, che si trattava di un accesso autorizzabile dal superiore gerarchico. E' vero, infatti, come sopra chiarito, che, per chi è autorizzato ad accedere al sistema, il reato può configurarsi anche semplicemente allorché ci si muova al di fuori dell'autorizzazione stessa, ma è del pari incontestabile che il principio è stato declinato con riguardo a casi in cui l'attività illecita aveva avuto a oggetto un atto rispetto al quale il dipendente è stato considerato funzionalmente estraneo. E' questo il profilo da esaminare nel rinnovato esame di merito, in cui 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, tenendo a mente, per un verso, che il predetto requisito ricorre quando si ritenga che vi sia stata la obiettiva violazione delle condizioni e dei limiti risultanti dalle prescrizioni impartite dal titolare del sistema per delimitarne l'accesso, compiuta nella consapevolezza di porre in essere una volontaria intromissione nel sistema in violazione delle regole imposte dal "*dominus loci*" ( Sez. 5, n. 33311 del 13/06/2016 Rv. 267403), e dall'altro che, come premesso, nel caso scrutinato, l'attività asseritamente abusiva ha avuto a oggetto un atto proprio del dipendente, compiuto nell'esercizio di una legittima prerogativa.

3. L'epilogo del presente giudizio di legittimità è l'annullamento della sentenza impugnata con rinvio per nuovo esame a Giudice di merito che dovrà scrutinare la questione posta dal ricorrente secondo le direttrici ermeneutiche sopra delineate.

**P.Q.M.**

Annulla la sentenza impugnata con rinvio per nuovo esame alla sezione promiscua della Corte di appello di Lecce

Così deciso in Roma, 17 maggio 2021

Il Consigliere estensore

Maria Teresa Belmonte



Il Presidente

Gerardo Saboneo

