L'ACQUISIZIONE DELLE CHAT PROVENIENTI DA SISTEMI CRIPTATI

SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

Corso P25006 – La disciplina delle intercettazioni: novità e problematiche

- 12 febbraio 2025 -

DOTT. MICHELE TORIELLO

SISTEMI CRIPTATI DI COMUNICAZIONE
1) BLACKBERRY

BLACKBERRY

In tema di intercettazione di comunicazioni telematiche, l'uso dell'algoritmo per la decriptazione della messaggistica con sistema "Blackberry" esclude la possibilità di alterazioni o manipolazioni dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici e concreti elementi di segno contrario.

Sez. 4, n. 30395 del 21 aprile 2022, Chianchiano, Rv. 283454-01

In tema di intercettazioni telefoniche, l'acquisizione della messaggistica, scambiata mediante sistema Blackberry, non necessita di rogatoria internazionale quando le comunicazioni siano avvenute in Italia, a nulla rilevando che per "decriptare" i dati identificativi associati ai codici PIN sia necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero.

Sez. 4, n. 49896 del 15 ottobre 2019, Brandimarte, Rv. 277949-02

In tema di intercettazioni della messaggistica scambiata con sistema Blackberry, la decriptazione del dato informatico è attività distinta dalla captazione e può essere svolta, ai sensi dell'art. 234-bis cod. proc. pen., mediante la mera richiesta alla società produttrice del sistema operativo di trasformare, tramite l'apposito algoritmo, i dati informatici in contenuti intellegibili.

Sez. 6, n. 18907 del 20 aprile 2021, Civale, Rv. 281819-01

SISTEMI CRIPTATI DI COMUNICAZIONE
2) ENCROCHAT

Encrochat Features

GUARANTEED ANONYMITY
No way to associate device or SIM card to customer account

CUSTOMISED ANDROID PLATFORM
Fully encrypted from power on. Focus on security and privacy. Simplified user settings.

DUAL OPERATING SYSTEM
Subscribers can now launch either a standard Android OS or the EncroChat OS. Two distinctive Operating Systems packaged with each device.

OVER-THE-AIR (OTA) SERVICE
Enhancements, patches, and features

MESSAGING PROTOCOL
The electronic equivalent of a regular conversation between two people in an empty room.

SIMPLIFIED VERIFICATION
Using our Notary verification process vastly simplifies the complexities of encryption for end users

MESSAGES THAT SELF-DESTRUCT
With our advanced burn a user can force wipe their own messages from another user's device using a timer countdown.

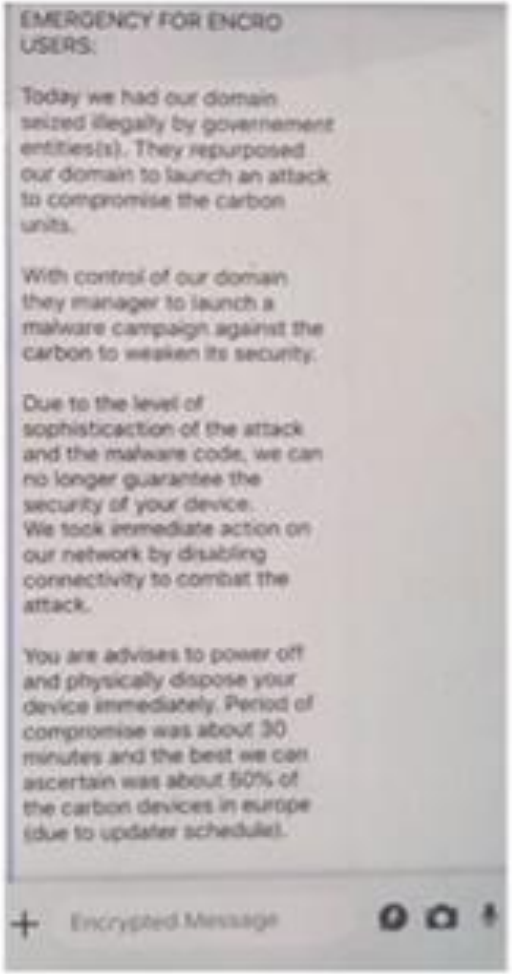
PANIC WIPE
From screen lock a user can type in a PIN and instantly wipe device's data.

PASSWORD WIPE
After a set amount of password attempts on device all data is wiped.

SECURE BOOT
Upon boot, the device internally checks itself to ensure no one has tampered with the system files.

ENCROCHAT

EncroChat


EMERGENCY FOR ENCRO USERS:
Today we had our domain seized illegally by governement entities(s). They repurposed our domain to launch an attack to compromise the carbon units.
With control of our domain they manager to launch a malware campaign against the carbon to weaken its security.
Due to the level of sophisticaction of the attack and the malware code, we can no longer guarantee the security of your device.
We took immediate action on our network by disabling connectivity to combat the attack.
You are advises to power off and physically dispose your device immediately. Period of compromise was about 30 minutes and the best we can ascertain was about 50% of the carbon devices in europe (due to updater schedule).
Encrypted Message

SISTEMI CRIPTATI DI COMUNICAZIONE
3) SKY-ECC

Our features protect your messages and privacy

SKY ECC has all the features you'd expect in a secure messaging platform and some features you didn't even realize you needed to be secure.

Self-destructing Messages

Set when a message will self-destruct or revoke a message immediately

Full-featured Group Chat

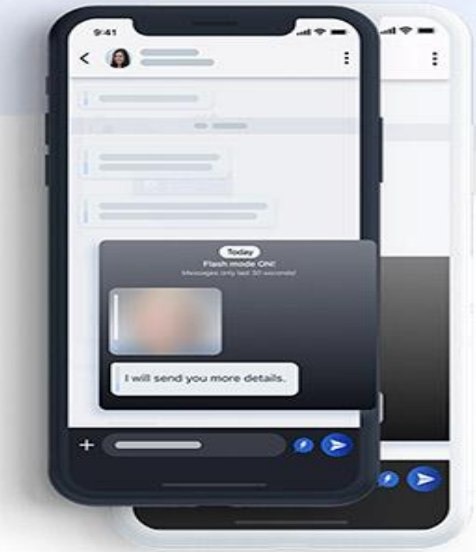
Keep everyone in sync, even large groups

Flash Messaging

Send messages that disappear 30 seconds after reading

Group Broadcast Messages

Send short updates to contact groups with a few taps



Share Images & Notes

Send notes, images, and contacts with control over downloading

Secure Audio Messages

Attach a secure audio clip to a message

Stealth Mode

In Stealth Mode SKY ECC becomes a fully-functional calculator

Secure Vault

Store images, chats, and notes in a protected file Vault

SKY-ECC

COUR D'APPEL DE DOUAI
Tribunal judiciaire de Lille

Cabinet de Marc CHEMIN
vice-président chargé de l'instruction

N° Parquet 19043000263
N° instruction JI CJIRSBC19000006
Identifiant justice 19004514491T

Pour Copie Conforme
Le Greffier

COMMISSION ROGATOIRE

INTERCEPTION DE CORRESPONDANCES PAR VOIE ELECTRONIQUE n°5

Nous, Marc CHEMIN, vice-président chargé de l'instruction, étant en notre cabinet au Tribunal judiciaire de Lille

Vu l'information suivie contre

X

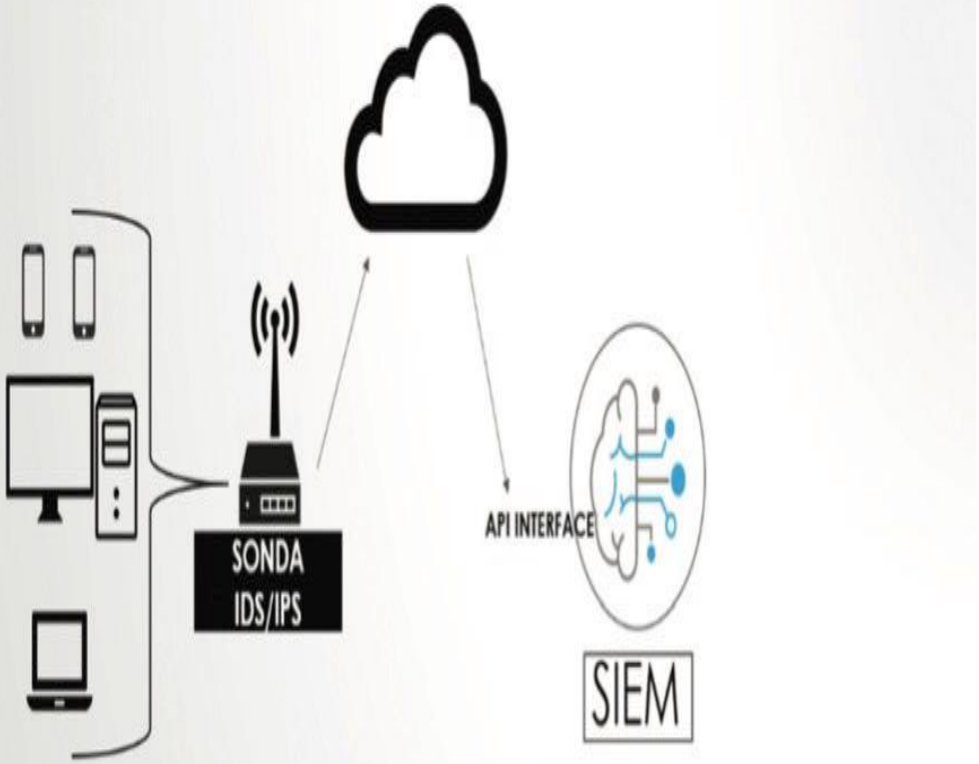
Mis en cause des chefs

- de FOURNITURE DE PRESTATIONS DE CRYPTOLOGIE VISANT A ASSURER DES FONCTIONS DE CONFIDENTIALITE SANS DECLARATION CONFORME faits commis courant janvier 2018 et jusqu'au 20 août 2019 à ROUBAIX et sur les départements du NORD et du PAS-DE-CALAIS, sur le ressort de la JIRS de LILLE
prévus par ART 35 §III ART 31 §I, ART.29 LOI 2004-575 DU 21/06/2004 ART 3, ART 4, ART 5, ART 8 DECRET 2007-663 DU 02/05/2007
et réprimés par ART 35 §III, §IV LOI 2004-575 DU 21/06/2004
- de PARTICIPATION A UNE ASSOCIATION DE MALFAITEURS EN VUE DE LA PREPARATION D'UN CRIME faits commis courant janvier 2018 et jusqu'au 20 août 2019 à ROUBAIX et sur les départements du NORD et du PAS-DE-CALAIS, sur le ressort de la JIRS de LILLE
prévus par ART 450-1 AL 1, AL 2 C PENAL
et réprimés par ART 450-1 AL 2, ART.450-3, ART 450-5 C PENAL
- de FOURNITURE D'UN MOYEN DE CRYPTOLOGIE N'ASSURANT PAS EXCLUSIVEMENT DES FONCTIONS D'AUTHENTIFICATION OU DE CONTROLE D'INTEGRITE SANS DECLARATION PREALABLE faits commis courant janvier 2018 et jusqu'au 20 août 2019 à ROUBAIX et sur les départements du NORD et du PAS-DE-CALAIS, sur le ressort de la JIRS de LILLE
prévus par ART 35 §I 1°, ART 30 §III ART.29 LOI 2004-575 DU 21/06/2004 ART 3, ART 4 ART 5 DECRET 2007-663 DU 02/05/2007
et réprimés par ART 35 §I 1° §IV LOI 2004-575 DU 21/06/2004
- d'IMPORTATION D'UN MOYEN DE CRYPTOLOGIE N'ASSURANT PAS EXCLUSIVEMENT DES FONCTIONS D'AUTHENTIFICATION OU DE CONTROLE D'INTEGRITE SANS DECLARATION PREALABLE faits commis courant janvier 2018 et jusqu'au 20 août 2019 à ROUBAIX et sur les départements du NORD et du PAS-DE-CALAIS, sur le ressort de la JIRS de LILLE
prévus par ART 35 §I 1 ART 30 §III ART 29 LOI 2004-575 DU 21/06/2004 ART 3, ART 4, ART 5 DECRET 2007-663 DU 02/05/2007
et réprimés par ART 35 §I 1° §IV LOI 2004-575 DU 21/06/2004
- de PARTICIPATION A ASSOCIATION DE MALFAITEURS EN VUE DE LA PREPARATION D'UN DELIT PUNI DE 10 ANS D'EMPRISONNEMENT faits commis courant janvier 2018 et jusqu'au 20 août 2019 à ROUBAIX et sur les départements du NORD et du PAS-DE-CALAIS, sur le ressort de la JIRS de LILLE
prévus par ART 450-1 AL 1, AL 2 C PENAL
et réprimés par ART 450-1 AL 2 ART 450-3, ART 450-5 C PENAL

Vu les articles 18, 81, 100, 100-1, 100-3 à 100-8, 151 et suivants du code de procédure pénale ;

Attendu que les investigations menées dans le cadre de la présente information judiciaire

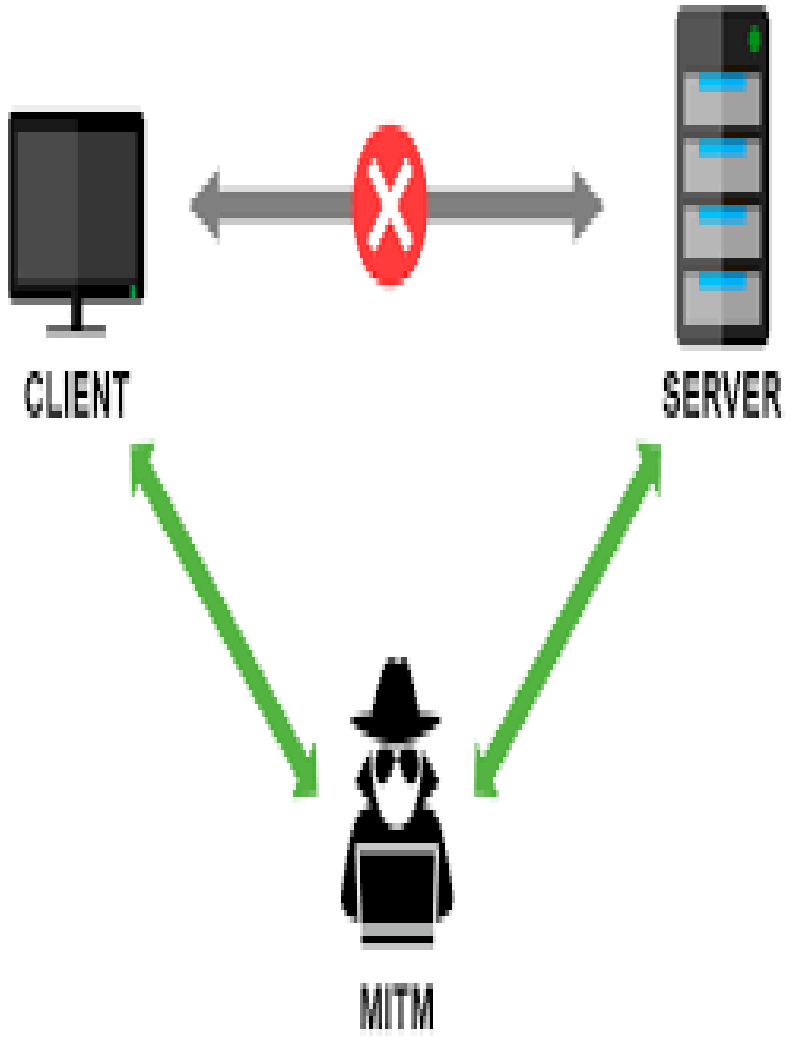
SKY-ECC



NETWORK ANALYSIS

Cosa ci permette di fare una sonda IDS/IPS:

- DNS Server all'interno della nostra rete protetta
- Supporto **DNSSEC**
- **Regole** DNS completamente **personalizzabili** per gruppi o singoli host
- **Blocco** pubblicità, domini **malware** e domini **phishing**
- Blocca domini gioco d'azzardo, social web e pornografia
- Panoramica dei dispositivi connessi alla rete wireless/wireline
- Monitoraggio statistiche DNS e log Suricata diciscuna sonda.



L'ORDINE EUROPEO DI INDAGINE

Direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014

Articolo 6 Condizioni di emissione e trasmissione di un OEI

1. L'autorità di emissione può emettere un OEI solamente quando ritiene soddisfatte le seguenti condizioni: a) l'emissione dell'OEI è necessaria e proporzionata ai fini del procedimento di cui all'articolo 4, tenendo conto dei diritti della persona sottoposta a indagini o imputata; e b) l'atto o gli atti di indagine richiesti nell'OEI avrebbero potuto essere emessi alle stesse condizioni in un caso interno analogo.

2. Le condizioni di cui al paragrafo 1 sono valutate dall'autorità di emissione per ogni caso.

Decreto legislativo 21 giugno 2017, n. 108

Principio di proporzione - art. 7

L'ordine di indagine non è proporzionato se dalla sua esecuzione può derivare un sacrificio ai diritti e alle libertà dell'imputato o della persona sottoposta alle indagini o di altre persone coinvolte dal compimento degli atti richiesti, non giustificato dalle esigenze investigative o probatorie del caso concreto, tenuto conto della gravità dei reati per i quali si procede e della pena per essi prevista.

LO STRUMENTO PROCESSUALE INTERNO DI RIFERIMENTO

Primo orientamento: dati informatici acquisibili all'estero ai sensi dell'art. 234 bis cod. proc. pen.

In tema di mezzi di prova, la messaggistica su "chat" di gruppo su sistema "Sky ECC", acquisita mediante ordine europeo di indagine da autorità giudiziaria straniera che ne ha eseguito la decriptazione, costituisce dato informativo documentale conservato all'estero, utilizzabile ai sensi dell'art. 234-bis cod. proc. pen., e non flusso comunicativo, non trovando applicazione la disciplina delle intercettazioni di cui agli artt. 266 e 266-bis cod. proc. pen. (In motivazione, la Corte ha chiarito che non rileva se i messaggi siano stati acquisiti dall'autorità giudiziaria straniera "ex post" o in tempo reale, poiché al momento della richiesta i flussi di comunicazione non erano in atto).

Sez. 4, n. 16347 del 5 aprile 2023, Papalia, Rv. 284563-01

LO STRUMENTO PROCESSUALE INTERNO DI RIFERIMENTO

Secondo orientamento: 254 bis cod. proc. pen. e 266 ss. Cod. proc. pen.

In tema di ordine europeo di indagine, l'oggetto dell'acquisizione all'estero della messaggistica criptata sulla piattaforma "SKY-ECC" non costituisce dato informatico utilizzabile ai sensi dell'art. 234-bis cod. proc. pen., sicché, in tale ipotesi, l'attività acquisitiva, se riguardante comunicazioni avvenute nella fase "statica", deve essere inquadrata nelle disposizioni in materia di perquisizione e sequestro e, in particolare, in quella di cui all'art. 254-bis cod. proc. pen., mentre se avente ad oggetto comunicazioni avvenute nella fase "dinamica", deve essere inquadrata nella disciplina degli artt. 266 e ss. cod. proc. pen. in materia di intercettazioni telematiche.

Sez. 1, n. 19082 del 13 gennaio 2023, Costacurta, Rv. 284440-01

LA RIMESSIONE ALLE SEZIONI UNITE

Sez. 3, ord. n. 47798 del 3 novembre 2023, Gjuzi

Sez. U, n. 23755 del 29 febbraio 2024, Gjuzi

Sez. 6, ord. n. 2329 del 15 gennaio 2024, Giorgi

Sez. U, n. 23756 del 29 febbraio 2024, Giorgi

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

In materia di ordine europeo di indagine, **la trasmissione del contenuto di comunicazioni scambiate mediante criptofonini**, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, **non rientra nell'ambito di applicazione dell'art. 234-bis cod. proc. pen.**, che opera al di fuori delle ipotesi di collaborazione tra autorità giudiziarie, **bensì nella disciplina relativa alla circolazione delle prove tra procedimenti penali, quale desumibile dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen.** (Fattispecie in tema di prove, costituite da messaggi scambiati su "chat" di gruppo mediante un sistema cifrato, già in possesso delle autorità competenti dello Stato di esecuzione).

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-01

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

In materia di ordine europeo di indagine, **le prove già in possesso delle autorità competenti dello Stato di esecuzione possono essere legittimamente richieste ed acquisite dal pubblico ministero italiano senza la necessità di preventiva autorizzazione da parte del giudice** del procedimento nel quale si intende utilizzarle.

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-02

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

In materia di ordine europeo di indagine, la sua emissione, da parte del pubblico ministero, diretta ad ottenere il contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, **non deve essere preceduta da autorizzazione del giudice italiano**, quale condizione necessaria a norma dell'art. 6 Direttiva 2014/41/UE, **perché tale autorizzazione, nella disciplina nazionale relativa alla circolazione delle prove, non è richiesta per conseguire la disponibilità del contenuto di comunicazioni già acquisite in altro procedimento**.

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-03

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

In materia di ordine europeo di indagine, la disciplina di cui all'art. 132 d.lgs. 30 giugno 2003, n. 196, relativa all'acquisizione dei dati concernenti il traffico di comunicazioni elettroniche e l'ubicazione dei dispositivi utilizzati, **si applica alle richieste rivolte ai fornitori del servizio, ma non anche a quelle dirette ad altra autorità giudiziaria che già detenga tali dati**, sicché, in questo caso, il pubblico ministero può legittimamente accedere agli stessi senza chiedere preventiva autorizzazione al giudice davanti al quale intende utilizzarli.

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-04

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

L'utilizzabilità del contenuto di comunicazioni scambiate mediante criptofonini, già acquisite e decrittate dall'autorità giudiziaria estera in un procedimento penale pendente davanti ad essa, e trasmesse sulla base di ordine europeo di indagine, **deve essere esclusa se il giudice italiano rileva che il loro impiego determinerebbe una violazione dei diritti fondamentali** previsti dalla Costituzione e dalla Carta dei diritti fondamentali dell'Unione Europea, e, tra questi, del diritto di difesa e della garanzia di un giusto processo, **fermo restando che l'onere di allegare e provare i fatti da cui inferire tale violazione grava sulla parte interessata.**

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-05

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

In materia di comunicazioni digitali, **l'impossibilità per la difesa di accedere all'algoritmo utilizzato nell'ambito di un sistema di comunicazioni per criptare il testo delle stesse non determina una violazione dei diritti fondamentali**, dovendo escludersi, **salvo specifiche allegazioni di segno contrario**, il pericolo di alterazione dei dati in quanto il contenuto di ciascun messaggio è inscindibilmente abbinato alla sua chiave di cifratura, ed una chiave errata non ha alcuna possibilità di decriptarlo anche solo parzialmente.

Sez. U, n. 23755 del 9 febbraio 2024, Gjuzi, Rv. 286573-06

I PRINCIPI AFFERMATI DALLE SEZIONI UNITE

(§ 9.2) «Nel sistema processuale italiano, infatti, il pubblico ministero e, più in generale, la parte che vi ha interesse possono chiedere ed ottenere la disponibilità di prove già formate in un procedimento penale al fine di produrle in un altro procedimento penale, senza necessità di alcuna autorizzazione preventiva da parte del giudice competente per quest'ultimo. Ciò anche nel caso di prove, come le intercettazioni di conversazioni o di comunicazioni, per la cui formazione è indispensabile la preventiva autorizzazione del giudice competente. Ovviamente, resta impregiudicato il potere del giudice competente per il procedimento penale nel quale le parti intendono avvalersi delle prove già separatamente formate o acquisite in altra sede di valutare se vi siano i presupposti per ammetterle ed utilizzarle ai fini della decisione. Questo assetto normativo si ricava con chiarezza dal sistema costituito dagli artt. 238 e 270 cod. proc. pen. e 78 disp. att. cod. proc. pen. L'art. 238 cod. proc. pen. detta le regole generali in tema di circolazione dei verbali di prove di altri procedimenti. La disciplina in esso contenuta, che si riferisce espressamente anche agli atti non ripetibili, non prevede, ai fini dell'acquisizione delle prove formate altrove, alcun intervento preventivo da parte del giudice del procedimento nel quale si vorrebbero utilizzarle. La norma si preoccupa unicamente di fissare condizioni per l'utilizzazione di prove provenienti da altri procedimenti; e, tra queste condizioni, non è ricompresa la previa autorizzazione del giudice. L'art. 270 cod. proc. pen., a sua volta, indica i requisiti per l'utilizzazione dei risultati delle intercettazioni di conversazioni o di comunicazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte. Anche questa disciplina, speciale rispetto a quella di cui all'art. 238 cod. proc. pen. perché riferita ad uno specifico mezzo di ricerca della prova, non prevede alcun intervento autorizzativo preventivo del giudice del procedimento di "destinazione", che abbia la funzione di autorizzare le parti interessate a procedere all'acquisizione di copia dei relativi atti».

CONSIDERAZIONI

Siamo in presenza di prove autonomamente raccolte dalle autorità straniere nell'ambito di procedimenti penali stranieri, sicché innanzitutto ci dobbiamo preoccupare di verificare che esse siano state acquisite nel rispetto della *lex loci*.

CONSIDERAZIONI

Siccome siamo in presenza di prove autonomamente raccolte dalle autorità straniere nell'ambito di procedimenti penali stranieri prima che le autorità giudiziarie italiane emettessero l'ordine europeo di indagine, per valutare la legittimità del procedimento che ha portato alla trasposizione di queste prove nei nostri procedimenti non dobbiamo guardare alla normativa interna in tema di formazione delle prove, ma a quella in tema di circolazione delle prove.

CONSIDERAZIONI

Il diritto di difesa trova piena estrinsecazione nel vaglio postumo rimesso al giudice del procedimento *ad quem*.

I difensori potrebbero innanzitutto contestare, ed hanno in effetti contestato, in via generale, il mancato rispetto dei principi di equivalenza, necessità e proporzionalità di cui all'art. 6 della Direttiva 2014/41/UE.

CONSIDERAZIONI

Altra questione che i difensori hanno sollevato attiene all'estensione dell'attività captativa posta in essere dalle autorità francesi.

*** Il nostro ordinamento consente un'intercettazione telematica che si sostanzi nel controllo continuo di un flusso di comunicazioni che intercorre su sistemi informatici o telematici, e nella apprensione del relativo contenuto (266 bis cod. proc. pen.): secondo Sez. 1, n. 12901 del 14 febbraio 2005, Palamara, Rv. 231591-01, «L'intercettazione di flussi telematici riconducibili ad un determinato utente mediante la procedura di monitoraggio del percorso, disposta dal gip, comporta la legittima captazione dei flussi informatici gestiti dal soggetto titolare di un determinato nome utente che contraddistingue sia l'*account* di posta elettronica che quello di connessione ..».**

*** La Corte Edu ha riconosciuto la liceità di captazione massive di dati, a condizione che vengano previste efficaci garanzie contro il rischio di abusi e di arbitrii nelle fasi di adozione della misura, della sua esecuzione e del controllo successivo (sentenze del 6 settembre 1978, Klass contro Germania; del 29 giugno 2006, Weber contro Germania; dell'1 luglio 2008, Liberty contro Regno unito; del 4 dicembre 2015, Zakharov contro Russia, che peraltro fanno riferimento non all'attività repressiva della polizia giudiziaria ma a quella preventiva dei servizi segreti).**

CONSIDERAZIONI

Un altro problema che in concreto si può porre riguarda la circostanza che le autorità francesi hanno come si è detto inoculato il captatore informatico all'interno dei due server, onde inviare ai criptofonini il malware grazie al quale si sono acquisite le due ultime chiavi di decriptazione mancanti.

1) Sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266-bis cod. proc. pen., effettuate mediante l'istallazione di un captatore informatico (c.d. *trojan horse*) all'interno di un computer collocato in un luogo di privata dimora. Sez. 5, n. 48370 del 30 maggio 2017, Occhionero, Rv. 271412-01

Motivazione (§ 9): la sentenza *Scurato* «si riferisce, dunque, in via esclusiva, alle 'intercettazioni tra presenti'. Con la conseguenza che il supremo organo nomofilattico non solo non ha escluso la legittimità dell'uso di tale strumento captativo per le intercettazioni tra presenti nei luoghi di privata dimora dove si stia svolgendo l'attività criminosa, ma soprattutto, ed è ciò che qui rileva, non l'ha esclusa per le ulteriori forme di intercettazione, tra cui quelle telematiche ex art. 266-bis, cod. proc. pen.».

CONSIDERAZIONI

2) In tema di intercettazioni telefoniche o ambientali, anche a mezzo di captatore informatico, non è causa di inutilizzabilità dei risultati di tali operazioni l'inosservanza delle disposizioni di cui all'art. 89 disp. att. cod. proc. pen., anche dopo le modifiche introdotte dal d.lgs. del 29 dicembre 2017, n. 216, essendo tale sanzione prevista solo per i casi tassativamente indicati dall'art. 271 cod. proc. pen. Sez. 5, n. 35010 del 30 settembre 2020, Monaco, Rv. 280398-02

Motivazione (§ 2.2) «le operazioni di collocazione e disinstallazione del materiale tecnico necessario per eseguire le captazioni [..] costituiscono atti materiali rimessi alla contingente valutazione della polizia giudiziaria, non essendo compito del pubblico ministero indicare le modalità dell'intrusione negli ambiti e luoghi privati ove verrà svolta l'intercettazione, poiché la finalità di intercettare conversazioni telefoniche e/o ambientali consente all'operatore di polizia la materiale intrusione, per la collocazione dei necessari strumenti di rilevazione, nei luoghi oggetto di tali mezzi di ricerca della prova; l'omessa documentazione delle operazioni svolte dalla polizia giudiziaria non dà luogo ad alcuna nullità od inutilizzabilità dei risultati delle intercettazioni ambientali [..] In altre parole, l'autorizzazione a disporre le operazioni di intercettazioni rende superflua l'indicazione delle modalità da seguire nell'espletamento dell'attività materiale e tecnica da parte della polizia giudiziaria, mentre la prova delle operazioni compiute nel luogo e nei tempi indicati dal giudice stesso e dal pubblico ministero è offerta dalla registrazione delle conversazioni intercettate».

CONSIDERAZIONI

Superato lo scoglio della equivalenza, necessità e proporzionalità, vi è ancora spazio per il diritto di difesa, potendo certamente essere contestata la irregolarità del procedimento acquisitivo -> principale deduzione difensiva -> non ci è stato consentito di analizzare il funzionamento del programma utilizzato per la decriptazione.

In tema di intercettazioni di flussi comunicativi, l'indisponibilità dell'algoritmo utilizzabile per la decriptazione dei dati informatici non determina alcuna lesione del diritto di difesa, atteso che l'interessato può avvalersi della procedura prevista dall'art. 268, commi 6 e 7, cod. proc. pen. per verificare il contenuto delle captazioni, ma non può anche pretendere un controllo diretto mediante l'utilizzo esclusivo e non mediato del programma di decriptazione.

Sez. 6, n. 14395 del 27 novembre 2018, Testa, Rv. 275534-01

CONSIDERAZIONI

In tema di intercettazione di comunicazioni telematiche, l'uso dell'algoritmo per la decriptazione della messaggistica con sistema "Blackberry" esclude la possibilità di alterazioni o manipolazioni dei testi captati, in quanto, secondo la scienza informatica, ne consente la fedele riproduzione, salvo l'allegazione di specifici e concreti elementi di segno contrario.

Sez. 4, n. 30395 del 21 aprile 2022, Chianchiano, Rv. 283454-01

In tema di mezzi di prova digitale, il sistema di diritto interno non garantisce alla difesa l'accesso agli algoritmi per la decodifica dei dati criptati, ma si limita a dettare garanzie procedurali a protezione della cd. "catena di custodia" nell'ottica dell'integrità probatoria, quali la necessità di un atto autorizzativo da parte di attori giudiziari qualificati, l'individuazione dei soggetti che possono acquisire e ritenere i dati e la disciplina della conservazione e consultazione degli stessi.

Sez. 6, n. 46390 del 26 ottobre 2023, Rosaci, Rv. 285494-01

CONSIDERAZIONI

In tema di prove digitali, l'indisponibilità della tecnologia di hackeraggio utilizzata per estrarre e mettere in chiaro la messaggistica criptata non determina alcuna lesione dei diritti di difesa, atteso che l'ordinamento interno non obbliga alla ostensione degli attrezzi virtuali con cui si sia ottenuta la decodifica di contenuti telematici, fatta salva la possibilità per l'imputato di allegare anomalie tecniche che facciano fondatamente dubitare della correttezza delle acquisizioni, e che depongano per l'inquinamento del risultato.

Sez. 6, n. 46482 del 27 settembre 2023, Bruzzaniti, Rv. 285363-04

CGUE 30 aprile 2024, C-670/22

77 Alla luce di tutte le considerazioni che precedono, occorre rispondere alla prima questione dichiarando che l'articolo 1, paragrafo 1, e l'articolo 2, lettera c), della direttiva 2014/41 devono essere interpretati nel senso che un ordine europeo di indagine inteso a ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione non deve essere adottato necessariamente da un giudice quando, in forza del diritto dello Stato di emissione, in un procedimento puramente interno a tale Stato, la raccolta iniziale di tali prove avrebbe dovuto essere ordinata da un giudice, ma competente ad ordinare l'acquisizione di dette prove è il pubblico ministero.

CGUE 30 aprile 2024, C-670/22

106 In considerazione della suesposta motivazione, occorre rispondere alle questioni seconda e terza dichiarando che l'articolo 6, paragrafo 1, della direttiva 2014/41 deve essere interpretato nel senso che esso non osta a che un pubblico ministero adotti un ordine europeo di indagine inteso ad ottenere la trasmissione di prove già in possesso delle autorità competenti dello Stato di esecuzione, qualora tali prove siano state acquisite a seguito dell'intercettazione, da parte di tali autorità, nel territorio dello Stato di emissione, di telecomunicazioni dell'insieme degli utenti di telefoni cellulari che permettono, grazie a un software speciale e ad un hardware modicato, una comunicazione cifrata da punto a punto, purché un tale ordine di indagine rispetti tutte le condizioni eventualmente previste dal diritto dello Stato di emissione per la trasmissione di tali prove in un caso puramente interno a detto Stato.

CGUE 30 aprile 2024, C-670/22

113 *In tertiis*, relativamente all'obiettivo dell'articolo 31 della direttiva 2014/41, dal considerando 30 di quest'ultima risulta che le possibilità di cooperare sulla base di tale direttiva in materia di intercettazione delle telecomunicazioni non dovrebbero essere limitate al contenuto delle telecomunicazioni, ma dovrebbero anche riguardare la raccolta di dati relativi al trafco e all'ubicazione associate a tali telecomunicazioni.

130 Ciò premesso, come risulta dai punti 104 e 105 della presente sentenza, non si può ignorare che l'articolo 14, paragrafo 7, della direttiva 2014/41 impone espressamente agli Stati membri di garantire, fatta salva l'applicazione delle norme procedurali nazionali, che, in un procedimento penale nello Stato di emissione, siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove ottenute mediante l'ordine europeo di indagine, il che comporta che un elemento di prova sul quale una parte non sia in grado di svolgere efcacemente le proprie osservazioni debba essere escluso dal procedimento penale.

CGUE 30 aprile 2024, C-670/22

131 Alla luce di tutti i motivi che precedono, occorre rispondere alla quinta questione dichiarando che l'articolo 14, paragrafo 7, della direttiva 2014/41 deve essere interpretato nel senso che esso impone al giudice penale nazionale di espungere, nell'ambito di un procedimento penale avviato a carico di una persona sospettata di atti di criminalità, informazioni ed elementi di prova se tale persona non è in grado di svolgere efficacemente le proprie osservazioni su tali informazioni ed elementi di prova e questi ultimi siano idonei ad influire in modo preponderante sulla valutazione dei fatti.

Per questi motivi (..)

5) L'articolo 14, par. 7, della direttiva 2014/41 deve essere interpretato nel senso che esso impone al giudice penale nazionale di espungere, nell'ambito di un procedimento penale avviato a carico di una persona sospettata di atti di criminalità, informazioni ed elementi di prova se tale persona non è in grado di svolgere efficacemente le proprie osservazioni su tali informazioni ed elementi di prova e questi ultimi siano idonei ad influire in modo preponderante sulla valutazione dei fatti.