

## **ARTICOLO DI PUNTOSICURO**

**Anno 25 - numero 5530 di Venerdì 22 dicembre 2023**

# **Il Regolamento 2023/1543 contro la criminalità informatica**

*Un regolamento europeo che aiuterà le forze dell'ordine a combattere i criminali informatici, ovunque essi si trovino, in Europa.*

Le varie basi operative e la mobilità, che caratterizzano l'attività dei criminali informatici, potranno essere meglio messe sotto controllo con la recente entrata in vigore del REGOLAMENTO (UE) 2023/1543 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 luglio 2023, relativo agli ordini europei di produzione ed agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive, a seguito di procedimenti penali.

Il 27 giugno 2023 l'Unione Europea ha formalmente adottato una nuova serie di regole, che offre indicazioni su come sia possibile alle forze dell'ordine acquisire dati, afferenti ad attività criminose, che si trovino in vari paesi europei. L'importanza di questo regolamento è sottolineata dal fatto che è stato pubblicato in tutte le lingue europee ed offre precise indicazioni a tutti i soggetti coinvolti, che ricevano richieste di conservazione e produzione di informazioni afferenti a crimini informatici.

Il grande vantaggio di questo regolamento è che esso permette alle forze dell'ordine di uno Stato di accedere direttamente ai dati che sono custoditi in un altro Stato, senza dover introdurre un'intermediazione giudiziaria.

Questo regolamento nasce dopo che l'esperienza ha mostrato come le indagini, soprattutto in caso di criminalità informatica, possano essere fortemente rallentate, per non dire addirittura bloccate, quando gli elementi di prova sono presenti in vari paesi europei.

Ad esempio, il fatto che Internet non abbia confini, il fatto che i malviventi usino sempre più spesso applicativi crittografici e che possano adottare delle tecniche, che consentono di rimanere anonimi, costituisce uno scenario che favorisce certamente di più l'attività dei malviventi, che quelle delle forze dell'ordine, incaricate di indagare su reati, prevalentemente di origine informatica.

Pubblicità

<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Quando i dati su cui indaga una procura della Repubblica, in Italia, sono conservati in altri paesi, ieri occorreva attivare un processo di collaborazione fra le diverse procure coinvolte, con tempistiche che erano in pieno contrasto con la celerità delle indagini, che rappresenta un aspetto essenziale delle indagini informatiche. Inoltre, può essere difficile provvedere al sequestro

di dati, se non si ha una sufficiente certezza del luogo dove tali dati si trovino e se non si è stabilito un accordo con le autorità giudiziarie competenti, per effettuare questo sequestro.

Un esempio clamoroso delle difficoltà, legate alle indagini su base europea, è descritto nelle indagini effettuate dopo l'attacco terroristico del 2016 a Bruxelles. Gli inquirenti trovarono grandi difficoltà nel reperire i dati afferenti ai soggetti coinvolti, che si trovavano in vari paesi e che erano conservati da gestori informatici, che avevano base in vari paesi.

Il regolamento stabilisce un quadro di riferimento per tutti paesi europei, circa le modalità con cui è possibile gestire le richieste di accesso a dati, durante indagini penali, che siano condotte da autorità giudiziarie che si trovino in altri paesi europei.

Il regolamento dà indicazioni sul tipo di richieste che possono essere presentate sia a forze dell'ordine di altri paesi, sia a service provider aventi sede in altri paesi. Il regolamento inoltre consente all'autorità giudiziaria di un paese di attivare un provvedimento di esibizione di dati, in qualunque paese si trovino.

Il provvedimento di esibizione viene contrassegnato dall'acronimo **EPO - European production order**.

Il regolamento introduce anche una severa tempistica perché il service provider obbedisca a questa richiesta, stabilendo un limite massimo di 10 giorni, che può essere ridotto addirittura ad otto ore, in casi particolarmente urgenti e debitamente motivati.

Un EPO deve soddisfare a tre condizioni:

- la richiesta deve essere necessaria e proporzionata, rispetto alle finalità dell'indagine penale in corso,
- la richiesta deve essere collegata ad un reato, per cui la pena applicabile sia di almeno tre anni,
- oppure la richiesta rientri nei tipi di violazione, che sono descritti nel regolamento.

Il regolamento introduce anche un altro documento, contrassegnato dall'acronimo **EPsO - European preservation order**. Questo documento obbliga un service provider a mantenere i dati richiesti per almeno 60 giorni. È evidente che l'obiettivo di questa disposizione è quello di impedire un'alterazione o cancellazione dei dati, sia accidentale, sia dolosa. Il periodo di conservazione dei dati può essere esteso di ulteriori 30 giorni.

Si deve inoltre prendere buona nota del fatto che la direttiva (EU) 2023/1544 obbliga ogni service provider, ovunque sia la sua sede, ma che opera in Europa, a designare un referente, al quale le autorità giudiziarie di tutta Europa possono indirizzare sia un EPO, sia un EPsO.

Invito tutti i lettori a leggere attentamente questo regolamento, perché le aziende, presso le quali essi operano, potrebbero essere destinatarie di queste richieste di documenti o dati, oppure perché sappiano che, ove stiano assistendo le autorità giudiziarie locali durante indagini di natura penale, di quali strumenti esse possono avvalersi, in caso di necessità. Inoltre, rinnovo la

raccomandazione di leggere attentamente non solo il regolamento, ma anche i "considerando", che spesso danno preziose indicazioni, atte a chiarire il significato di specifici articoli del regolamento.

[REGOLAMENTO \(UE\) 2023/1543 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 12 luglio 2023 relativo agli ordini europei di produzione e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e per l'esecuzione di pene detentive a seguito di procedimenti penali.](#) (pdf)

**Adalberto Biasiotti**



Licenza [Creative Commons](#)

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

---

[www.puntosicuro.it](http://www.puntosicuro.it)