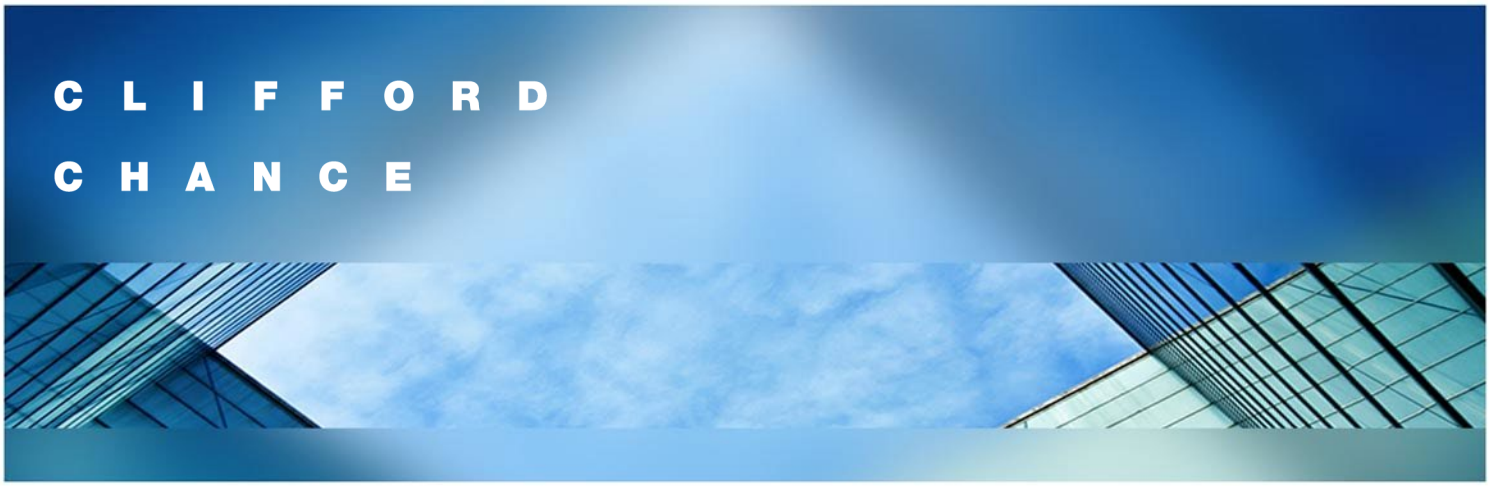

A NEW FRONTIER IN THE FIGHT AGAINST CYBERCRIME: THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION

On 12 May 2022 in Strasbourg, 22 Countries Members of the European Council, including Italy, ratified the **Second Additional Protocol to the Convention on cybercrime** (the "**Budapest Convention**") **on enhanced cooperation and disclosure of electronic evidence** (the "**Second Protocol**").

Key issues

- Direct and immediate channels for co-operation between States and service providers to obtain information on registrants of domain names, subscribers and traffic data
- Special procedure in emergencies
- Mechanisms for mutual assistance
- Guarantees as to the protection of personal data

Given the ever-growing range of cybercrimes, increasingly complex and "without borders", Judicial Authority constantly faces difficulties in obtained the required electronic evidence, which is volatile by its very nature, when it is located in foreign jurisdictions. Traditional cooperation mechanisms, for example international letters rogatory, have often been ineffective, and are always a labour-intensive process.

Therefore, the Second Protocol aims to create **common norms,** at the international level, to **strengthen cooperation** in fighting cybercrime and in collecting **electronic evidence** in connection with criminal investigations or proceedings**.**

The Second Protocol requires that the signatory Countries create specific rapid and direct communication channels between all the state authorities involved as well as between the state authorities and the private sector, such as online service providers located in foreign jurisdictions, so as to allow collection and disclosure, easily and quickly, of information relating to, for example, registration of domain names, subscribers and traffic data.

THE NEW PROCEDURES UNDER THE SECOND PROTOCOL

The Second Protocol provides that, in the context of criminal investigations or proceedings pending before the courts of a signatory Country, the Country itself will be able – through the competent authorities:

- to send directly to an **entity that register domain names,** located in another signatory Country, **a request** for information in its possession or control, if the information is necessary to identify or to contact the registrant of a domain name (Art. 6 of the Second Protocol);
- to send directly to an **online service provider** in the territory of another signatory Country **an order** to obtain the disclosure of specified, stored

subscriber information, in the service provider's possession or control, where the subscriber information is needed for the criminal proceedings pending before the courts of the requesting Country (Art. 7 of the Second Protocol).

If the online service provider does not comply in a timely manner or fails to comply, the Second Protocol provides for the authorities of the Country in which the "defaulting" service provider is located to issue an order requiring the service provider to disclose a subscriber's information and traffic data, in its possession or control, as requested by the requesting Country (Art. 8 of the Second Protocol).

Moreover, the Second Protocol also creates out a novel, **expedited disclosure process for use in emergencies,** to be serviced through the "Point of Contact" identified by each State (as already provided for under Article 35 of the Budapest Convention), which is to be open 24 hours a day, seven days a week, and will receive and transmit requests seeking immediate assistance in obtaining from a service provider the expedited disclosure in its possession or control (Art. 9 of the Second Protocol).

Finally, the Second Protocol sets forth specific **guarantees for the protection of personal data**. Thus, all the Countries in the European Union will need to harmonise legislation on the basis of the already existing principles governing data protection (such as the European Law Enforcement Directive, governing the protection of personal data in judicial and police activities).

After ratification, the signatory Countries will need to adopt adequate measures to render effective the cooperation procedures set out in the Second Protocol. According to Article 5 of the Second Protocol, the cooperation procedures will be applicable, whether (or not) the States have entered into individual treaties for mutual assistance.

WHERE IS EUROPE HEADING?

The signing of the Second Protocol is part of the significant recent evolution, mainly at the European level, that has led to an overall strengthening of the measures for cooperation between States, to fight criminality with the highest possible efficacy. These measures include, for example, the introduction of the European Arrest Warrant and the European Investigation Order, and the very recent creation of an European Public Prosecutor's Office.

Additionally, the ratification of the Second Protocol is a major step forward in terms of strict **prevention of cybercrime as well as in terms of evolution of electronic investigations:** both of which are priorities for the European Union.

The role of electronic evidence, indeed, has become more and more central not only in cybercrime proceedings but also in proceedings relating to other crimes, such as money laundering – which although not properly a "cybercrime" is moving towards a highly digital dimension. Against this backdrop, "traditional" cooperation instruments such as international letters rogatory, or the mere reliance on the choices made by service providers, through agreements, can no longer guarantee an adequate, rapid and effective large-scale response. The world wide web has no borders, it is supra-national; and this must be kept in mind at all times.

In light of the constant, characteristic evolution, therefore, in the "European scenario", i.e. broadly defined, given that the Budapest Convention and the

Second Protocol affect all Member States of the Council of Europe and not only the European Union Member States (Countries that have ratified the Second Protocol include, for example, the United Kingdom), it becomes essential to rely on highly specialised legal advisors, with solid cross-border experience for:

- on one hand, victims of cybercrime (or other crimes); for the judicial authorities to request in a timely and effective manner the assistance of all Europe-wide and cross-border cooperation channels and instruments available under the new legislation, especially so as to obtain those elements of evidence essential in the context of criminal investigations and proceedings even when such evidence in is foreign jurisdictions;
- on the other hand, addressees of requests from foreign authorities, sent pursuant to the new European and cross-border legislation, so as to best manage such requests, providing adequate responses in the shortest time possible. Because of the procedures introduced by the Second Protocol, this scenario will become increasingly frequent, especially for managers of electronic platforms.

More generally, the Second Protocol is part of a broader range of initiatives that aim to ensure that online activities are lawful. For example, the draft 'Digital Services Act' ("**DSA**"), which is expected to become applicable starting from 2024. The objective of the DSA is to make safer the "digital space" in Europe, setting forth stringent obligations for information services – such as online marketplaces, app stores and social networks – in an attempt to fight fake news and misinformation, the marketing of counterfeit products, and the distribution of illegal contents. Similarly to the GDPR, the DSA provides for fines of up to 6% of the offender's global annual revenues.

CONTACTS

Giuseppe Principato
Counsel

T +39 02 8063 4214
M +39 337 1140405
E giuseppe.principato@cliffordchance.com

Laura Scaramellini
Senior Associate

T +39 02 8063 4297
M +39 337 1402082
E laura.scaramellini@cliffordchance.com

Giovanni Minucci
Associate

T +39 02 8063 4027
M +39 331 6672450
E Giovanni.Minucci@cliffordchance.com

Giada Scarnera
Associate

T +39 02 8063 4224
M +39 360 1012788
E giada.scarnera@cliffordchance.com