CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

WHATSAPP ET LE CHIFFREMENT DE BOUT EN BOUT ET LA SÉCURITÉ: RÉFLEXIONS SUR LA PROCÉDURE PÉNALE.

Comme est-ce que la sécurité de l'application de messagerie la plus populaire et utilisée par plus d'un milliard d'utilisateurs va changer? Peut-on vraiment parler de la protection de la confidentialité? Comment les relations entre l'autorité judiciaire et les procédures pénales vont changer?

di **Simone Lonchiar**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Giovedì 2 Giugno 2016

CamminoDiritto.it
ISSN 2421-7123

Il y a quelques jours sur WhatsApp est apparu le texte suivant: 'Les messages que vous envoyez dans cette discussion et les appels sont désormais protégés avec le chiffrement de bout en bout'.

Qu'est-ce que cela signifie? Ce chiffrement spécial permet seulement aux utilisateurs intéressés (émetteur et récepteur), d'avoir la permission de lire et d'agir pour ce qui concerne les messages de la conversation en commun. En matière de sécurité, cette nouvelle technologie permet au message de n'être pas intercepté pendant toute la durée de la transmission. WhatsApp lui-même n'a pas la permission d'agir sur les messages vocaux ou d'autre type.

WhatsApp est l'application de messagerie pour smartphones avec plus d'un milliard d'utilisateurs actifs. Elle a été créée par Jan Koum et Brian Acton en 2009, et elle a ensuite été acquise par Mark Zuckerberg, PDG de Facebook, le 19 Février 2014.

Pourquoi ce changement?

Le chemin a été long et détourné et l'une de principales raisons de l'introduction de cette nouvelle fonctionnalité est l'ajustement avec d'autres applications ayant la même fonction de messagerie instantanée, en particulier avec Telegram.

Telegram, en fait, a considérablement augmenté ses utilisateurs en quelques mois grâce à l'offre de meilleures garanties sur la confidentialité. Ces nouvelles garanties ne sont pas les seules fonctions supplémentaires (voir aussi le «bot») que Telegram offre de plus que WhatsApp.

Comment fonctionne la technologie de chiffrement bout en bout?

Pour les non-spécialistes, on peut exprimer le concept de chiffrement de bout en bout, en pensant à son équivalent 'de point à point': les clefs de lecture sont seulement dans les dispositifs de l'émetteur et du récepteur et dans le canal d'échange; de cette façon les messages échangés entre deux personnes sont cryptés à partir du moment où on appuie sur Entrée.

CamminoDiritto.it
ISSN 2421-7123

Ce cryptage ne permet pas aux méchants ou aux autorités de pirater ou de s'adresser à la plate-forme, en empêchant l'acquisition des informations. Il faut souligner que ce protocole, adopté par l'application, ne protège pas les données stockées dans le dispositif.

Pour une meilleure vue d'ensemble, le site de WhatsApp et ses applications dans la section 'Sécurité' ont mis au point une explication claire et animée, même pour les utilisateurs qui ont une connaissance limitée du langage technologique.

Qu'est ce qui a changé et qu'est ce que cela signifie pour les utilisateurs?

Comme indiqué ci-dessus, le chiffrement de bout en bout est réservé à tous les utilisateurs de WhatsApp qui ont mis à jour l'application. Cela signifie que celui qui a l'application dépassée, il la devra mettre à jour pour être capable d'envoyer et recevoir les messages et les appels.

Le chiffrement, a-t-il vraiment résolu le problème de la confidentialité?

À cette question clé, qui peut être considérée comme le véritable cœur du problème, a répondu Luigi Martino, assistant de recherche dans les politiques de TIC et de la cyber-sécurité à l'Université de Florence. Dans une interview avec Cyber Affaires il a déclaré que: «[...] ne signifie pas que le contenu du message ne reste pas à la disposition de WhatsApp, qui possède et contrôle les serveurs sur lequel ces données sont stockées.» '. Il continue avec une question qui nous fait penser: «Voici ce que nous devrions nous demander pour ce qui concerne la protection de la confidentialité: qui sont, aujourd'hui, les propriétaires des conversations et des données transitant par le réseau? C'est nous ou les fournisseurs des services? ».

L'interception informatique et télématique dans la procédure pénale en Italie.

L'interception télématique est dirigée pour apprendre la transmission d'un flux de communication de forme réservée, en conformité avec les garanties prévues par l'art. 15 Const. et l'art. 8 CEDH.

CamminoDiritto.it
ISSN 2421-7123

Les interceptions des communications informatiques et télématiques sont réglementées par l'art. 266-bis du CPP:

«Dans les procédures relatives aux crimes indiquées à l'art. 266, ainsi qu'aux crimes qui ont été commis par l'utilisation de technologies informatiques ou télématiques, il est permis l'interception du flux de communication lié aux systèmes informatisés ou télématiques, donc entre plusieurs systèmes ». Cette définition peut également être étendue à tous les crimes commis par l'utilisation des technologies informatiques.

La perquisition informatique a été introduite dans le Code de procédure pénale à l'art. 8 paragraphe 2 de la loi 48/08, elle est réglementée par l'art. 247 paragraphe 1 bis CPP et elle prévoit que:

«Quand il y a des raisons de croire que des données, des informations, des programmes ou des pistes informatiques encore pertinentes au crime sont stockées dans un système informatique ou télématique, même s'ils sont protégés par des mesures de sécurité, on en dispose la perquisition, en utilisant des mesures techniques visant à assurer la conservation des données originales et afin d'éviter leur manipulation».

Avant d'entreprendre la perquisition, l'art. 247 alinéa 1-bis CPP, exige l'adoption de "mesures techniques" visant à "assurer la conservation des données originales et en empêcher leur modification", afin d'assurer l'acquisition et le stockage de l'élément de preuve. Avant de pouvoir utiliser cet outil de recherche pour la preuve, on doit adopter chaque garantie visant à protéger l'inviolabilité du domicile "informatique", compris comme "espace récipient" de toutes les données informatiques appartenant à la personne. À cet espace on étend la protection de la confidentialité individuelle.

Donc, à la lumière des nouveautés qui ont été introduites, les conversations échangées entre les utilisateurs de WhatsApp ne seront plus utilisées à des fins de preuve.

Le chiffrement de bout en bout et la relation avec l'autorité judiciaire

Le chiffrement de bout en bout signifie, par conséquent, que le même WhatsApp et les parties tiers ne peuvent pas lire les messages ou écouter les appels et les messages vocaux. Crypter les communications aujourd'hui peut être vital pour les personnes qui vivent dans pays contrôlés par régimes totalitaires et violents, pays où l'interception de messages

CamminoDiritto.it
ISSN 2421-7123

indésirables au régime déterminent des risques pour la vie ou l'emprisonnement.

Le chiffrement de bout en bout ne permettra plus à WhatsApp la possibilité de divulguer le contenu des messages, même si les autorités l'exigent, donc dans cette façon le citoyen aura une plus grande protection contre les cybercrimes. Toutefois, selon Andrea Zapparoli Manzoni, membre du Clusit, l'association italienne pour la sécurité informatique: «Il faut se rappeler que la protection des données transitant est seulement une composante d'une stratégie globale de sécurité et que le chiffrement de messages par lui-même, il ne peut pas garantir la sécurité absolue des communications», car «il y a deux autres éléments à prendre en considération: la sécurité de l'appareil fixe ou mobile sur lequel fonctionne l'application et la sécurité de l'application elle-même. Pour eux, il y a des menaces réelles, qui ne sont nullement atténué par l'adoption de chiffrement sur le canal de transmission».

Néanmoins, il y a des exceptions. Dans un article paru dans La Repubblica le 1er Mars 2016, on lit en effet que BlackBerry ne s'est pas aligné avec le choix d'Apple et WhatsApp et il a remis aux juges de Turin les conversations en commun qui ont coincé certains criminels. Il s'agit actuellement de discussions échangées par l'application «interne» de BlackBerry, une application qui peut être utilisée seulement entre les utilisateurs qui possèdent téléphones mobiles de cette marque. Le problème qui se pose, cependant, est que ces conversations en commun, selon les avocats qui défendent la gang de trafiquants de drogue, ne peuvent pas être utilisées parce qu'elles n'ont pas été directement 'interceptées' par l'autorité judiciaire.
