SEMDOC

Statewatch European Documentation &
Monitoring Centre on justice and home
affairs in the European Union

PO Box 1516, London N16 0EW, UK
tel: 0181 802 1882 (00 44 181 802 1882)
fax: 0181 880 1727 (00 44 181 880 1727)

10571/2/94

31 215

REV 2 (f)
RESTREINT

ENFOPOL 150

RESULTATS DES TRAVAUX

du : Groupe "Coopération policière"

au : Comité K.4

n° doc. préc. : 10571/94 ENFOPOL 150 + COR 1

Objet : Projet de résolution du Conseil relative aux spécifications internationales concernant
la surveillance légale des télécommunications

1. Lors de sa réunion des 9, 10 et 11 novembre 1994, le Comité K.4 avait chargé le groupe "Coopération policière" de régler les questions en suspens concernant le projet de résolution du Conseil visé en objet.
 2. Le 23 novembre 1994, un accord s'est fait au sein du groupe "Coopération policière" sur les questions qui restaient en suspens. En conséquence, les délégations ont suggéré que le texte du projet de résolution du Conseil susmentionné, tel qu'il figure dans le présent document, soit soumis au Comité K.4 en vue de son adoption par le COREPER et le Conseil en point "I/A".
-

Projet de
**RESOLUTION DU CONSEIL
DE L'UNION EUROPEENNE**
du

**relative aux spécifications internationales concernant
la surveillance légale des télécommunications**

LE CONSEIL DE L'UNION EUROPEENNE,

vu le traité sur l'Union européenne,

rappelant l'article K.1 point 9 et l'article K.2 paragraphe 2 de ce traité,

réaffirmant la nécessité de respecter, dans la mise en oeuvre des mesures d'interception des télécommunications, le droit des personnes physiques au respect de la vie privée consacré par les législations nationales territorialement applicables,

conscients du fait que ce respect soulève des difficultés juridiques et techniques spécifiques, compte tenu des progrès technologiques,

déterminés à identifier et à surmonter ces difficultés dans la mise en oeuvre des spécifications reprises en annexe dans le respect des droits de l'homme et du principe de la protection des données,

considérant les dispositions des législations des Etats membres permettant de limiter le secret des communications et d'intercepter, dans certaines conditions, les télécommunications ;

considérant que la surveillance légale des télécommunications est un outil important pour la protection des intérêts nationaux, notamment la sécurité nationale et l'instruction en matière de criminalité grave ;

considérant que cette surveillance ne peut être effectuée que dans la mesure où les dispositions techniques nécessaires ont été prises ;

considérant que, selon une décision prise par les ministres TREV I en décembre 1991, une étude devrait être effectuée en ce qui concerne les conséquences de l'évolution juridique et technique et de l'évolution du marché dans le domaine des télécommunications à l'égard des différentes possibilités d'interception et en ce qui concerne les mesures à prendre afin de faire face aux problèmes qui ont surgi,

ADOpte LA PRESENTE RESOLUTION :

1. Le Conseil note que les "Spécifications" d'une surveillance légale des télécommunications, qui figurent en annexe, constituent un condensé important des besoins des autorités compétentes pour la réalisation technique des mesures de surveillance légale, notamment dans les systèmes modernes de télécommunications.

2. Le Conseil estime que les spécifications précitées doivent être prises en considération lors de la définition et de l'exécution de la surveillance légale des télécommunications et demande aux Etats membres d'inviter les ministres responsables des télécommunications à soutenir cette position et à coopérer avec les ministres de la Justice et des Affaires intérieures, afin d'appliquer ces spécifications en ce qui concerne les opérateurs de réseaux et les fournisseurs de services.

Par le Conseil de l'Union européenne,
Le président

SPECIFICATIONS

La présente section expose les spécifications des services autorisés relatives à l'interception légale des télécommunications. Ces spécifications sont soumises à la loi nationale et doivent être interprétées conformément aux politiques nationales applicables.

Les définitions figurent dans le glossaire en annexe.

1. Les services autorisés doivent avoir accès à l'ensemble des télécommunications transmises ou que l'on a fait transmettre vers le numéro ou à partir du numéro ou autre identificateur du service cible utilisé par le sujet de l'interception. Les services autorisés doivent également avoir accès aux données afférentes à l'appel qui sont émises pour le réaliser.
 - 1.1. Les services autorisés doivent pouvoir intercepter les communications lorsque le sujet de l'interception se déplace à l'intérieur d'un système de télécommunication de façon temporaire ou permanente.
 - 1.2. Les services autorisés doivent avoir accès aux télécommunications lorsque le sujet de l'interception utilise des procédés pour transférer les appels vers d'autres services de télécommunication ou d'autres équipements de terminal, y compris les appels qui traversent plus d'un réseau ou qui sont traités par plus d'un opérateur de réseau ou fournisseur de services avant d'aboutir.
 - 1.3. Les télécommunications effectuées par le sujet de l'interception ou qui lui sont adressées doivent être accessibles aux services autorisés à l'exclusion de toutes les autres télécommunications qui n'ont pas de rapport avec le service cible précisé dans l'autorisation d'interception.
 - 1.4. Les services autorisés doivent avoir accès aux données afférentes aux appels telles que :
 - 1.4.1. Caractéristiques du signal d'accès
 - 1.4.2. Numéro appelé pour les communications de sortie même si la communication ne peut être établie
 - 1.4.3. Numéro de l'appelant pour les communications d'entrée même si la communication ne peut être établie
 - 1.4.4. Tous les signaux émis par la personne faisant l'objet de la surveillance, y compris les chiffres émis après la communication pour effectuer des audioconférences ou des transferts d'appels
 - 1.4.5. Début, fin et durée de la communication
 - 1.4.6. Destination réelle et numéros intermédiaires si l'appel a été transféré.

- 1.5. Les services autorisés doivent disposer d'informations très précises sur la localisation géographique connue du réseau en ce qui concerne les utilisateurs mobiles.
- 1.6. Les services autorisés doivent connaître les données concernant le service spécifique utilisé par le sujet de l'interception et les paramètres techniques de ce type de communication.
2. Les services autorisés doivent avoir des possibilités de surveillance en temps réel et à temps plein pour les interceptions de transmissions de télécommunications. Des données suffisantes afférentes aux appels doivent également être fournies en temps réel. Si des données complémentaires afférentes à l'appel ne peuvent être fournies en temps réel, les services autorisés doivent disposer de ces données dans les meilleurs délais dès la fin de l'appel.
3. Les opérateurs de réseaux ou les fournisseurs de services doivent procurer aux services autorisés une ou plusieurs interfaces à partir desquelles les communications interceptées peuvent être transmises à leurs installations de surveillance. Ces interfaces doivent faire l'objet d'un accord entre les autorités qui interceptent les communications et les opérateurs de réseaux ou les fournisseurs de services. Les autres questions relatives à ces interfaces seront traitées selon les pratiques admises dans les différents pays.
 - 3.1. Les opérateurs de réseaux ou les fournisseurs de services doivent transmettre aux services autorisés les données afférentes à l'appel qui proviennent du service cible et le contenu de l'appel de façon à permettre d'établir un rapport précis entre les données afférentes à l'appel et le contenu de celui-ci.
 - 3.2. Le format de transmission des communications interceptées vers une installation de surveillance doit généralement être disponible aux services autorisés. L'accord sur ce format se fera pays par pays.
 - 3.3. Si les opérateurs de réseau ou les fournisseurs de services procèdent au codage, à la compression ou au chiffrement des données transmises, les interceptions correspondantes doivent être fournies en clair aux services autorisés par les opérateurs de réseau ou les fournisseurs de services.
 - 3.4. Les opérateurs de réseaux ou les fournisseurs de services doivent être capables de transmettre les communications interceptées à l'installation de surveillance des services autorisés au moyen de connections fixes ou "commutées".
 - 3.5. La transmission des communications interceptées aux installations de surveillance doit être conforme aux exigences de sécurité applicables.
4. Les interceptions doivent être mises en oeuvre de manière à ce que ni la cible de l'interception ni toute autre personne non autorisée ne soit au courant des modifications effectuées pour exécuter l'ordre d'interception. En particulier, le sujet de l'interception ne doit pas remarquer de modification dans la prestation du service cible.

5. L'interception doit être conçue et mise en oeuvre de façon à empêcher toute utilisation non autorisée ou abusive et à sauvegarder les informations concernant l'interception.
- 5.1. Les opérateurs de réseaux ou fournisseurs de services doivent protéger les informations qu'ils détiennent sur la nature et le nombre des interceptions qu'ils réalisent ou ont réalisées et ne doivent pas divulguer pas les informations liées à la méthode d'interception.
- 5.2. Les opérateurs de réseaux ou les fournisseurs de services doivent veiller à ce que les communications interceptées soient exclusivement transmises au service de surveillance désigné dans l'autorisation d'interception.
- 5.3. Conformément aux exigences nationales, les services autorisés peuvent exiger des opérateurs de réseaux ou des fournisseurs de services qu'ils tiennent un registre adéquatement protégé des mesures d'interception.
6. Sur la base d'une enquête légale et avant la réalisation de l'interception, les services autorisés demandent aux opérateurs de réseaux ou fournisseurs de services (1) de leur fournir l'identité du sujet de l'interception, le numéro de service ou tout autre signe distinctif, (2) des informations sur les services et les caractéristiques du système de télécommunications utilisé par le sujet de l'interception et fourni par les opérateurs de réseaux ou les fournisseurs de services et (3) des informations sur les paramètres techniques de la transmission à l'installation de surveillance de services autorisés.
7. Au cours de l'interception, les services autorisés peuvent exiger que les opérateurs de réseaux ou les fournisseurs de services fournissent des informations et/ou de l'aide pour vérifier que les communications reçues au point d'interception sont bien les communications associées au service cible. Le type d'information et/ou d'aide requis dépendra des pratiques admises dans chaque pays.
8. Les opérateurs de réseaux ou les fournisseurs de services doivent prendre des mesures pour la mise en oeuvre d'un certain nombre d'interceptions simultanées. Des interceptions multiples peuvent être exigées pour un unique service cible afin de permettre la surveillance par plusieurs services autorisés. Dans ce cas, les opérateurs de réseaux ou les fournisseurs de services doivent prendre des précautions pour sauvegarder l'identité des services de surveillance et assurer la confidentialité des enquêtes. Le nombre maximum d'interceptions simultanées pour une population donnée d'abonnés sera conforme aux exigences nationales.
9. Les opérateurs de réseaux ou les fournisseurs de services doivent réaliser les interceptions dans les meilleurs délais (en cas d'urgence, en quelques heures ou quelques minutes). Le temps de réaction exigé par les services autorisés dépendra du pays et du type de service cible à intercepter.

10. Pendant la durée de l'interception, la fiabilité des services auxiliaires de l'interception doit au moins être équivalente à celle des services cible fournis au sujet de l'interception. La qualité de service des communications interceptées transmises à l'installation de surveillance doit répondre aux normes d'exécution des opérateurs de réseaux ou des fournisseurs de services.
-