CONSEIL DE L'EUROPE
COMITÉ DES MINISTRES

RECOMMANDATION N° R (95) 13

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES RELATIVE AUX PROBLÈMES DE PROCÉDURE PÉNALE LIÉS À LA TECHNOLOGIE DE L'INFORMATION

(adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres)

Le Comité des Ministres, en vertu de l'article 15.*b* du Statut du Conseil de l'Europe,

Rappelant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Eu égard au développement sans précédent de la technologie de l'information et de son application dans tous les secteurs de la société contemporaine ;

Réalisant que le développement des systèmes électroniques d'information va accélérer la transformation de la société traditionnelle en une société de l'information en créant un nouvel espace pour tout type de communication et de relation ;

Conscient de l'impact de la technologie de l'information sur la manière dont la société est organisée et sur la façon dont les individus communiquent et se mettent en relation ;

Conscient du fait qu'une partie croissante des relations économiques et sociales aura lieu à travers ou à l'aide de systèmes électroniques d'information ;

Préoccupé par le risque que les systèmes électroniques d'information et l'information électronique puissent également être utilisés pour commettre des infractions criminelles ;

Préoccupé par le fait que les preuves d'infractions pénales peuvent être stockées et transmises par le biais de ces systèmes ;

Notant que les lois de procédure pénale des Etats membres ne prévoit pas encore souvent les pouvoirs appropriés pour perquisitionner dans ces systèmes et y recueillir des preuves au cours des enquêtes pénales ;

Rappelant qu'au vu du développement de la technologie de l'information le manque de pouvoirs spéciaux appropriés peut porter atteinte à la bonne exécution des fonctions assignées aux autorités chargées de l'enquête ;

Reconnaissant la nécessité d'adapter les moyens légaux dont disposent les autorités chargées de l'enquête en vertu des lois de procédure pénale au caractère spécifique des enquêtes dans les systèmes électroniques de l'information ;

Préoccupé par le risque potentiel que les Etats membres ne soient pas en mesure de fournir une entraide judiciaire de manière adéquate lorsqu'ils sont requis de recueillir des preuves électroniques, sur leur territoire, dans des systèmes électroniques d'information ;

Persuadé de la nécessité de renforcer la coopération internationale et de parvenir à une meilleure compatibilité des lois de procédure pénale en la matière ;

Rappelant la Recommandation n° R (81) 20 relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'admissibilité des reproductions de documents et des enregistrements informatiques, la Recommandation n° R (85) 10 sur les commissions rogatoires pour la surveillance des télécommunications, la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police et la Recommandation n° R (89) 9 sur la criminalité informatique,

Recommande aux gouvernements des Etats membres:

i. de s'inspirer, lorsqu'ils révisent leurs législation et pratiques internes, des principes qui se trouvent en annexe à cette recommandation; et

ii. de faire connaître ces dispositions aux autorités chargées de l'enquête et à d'autres services professionnels, en particulier dans le secteur de la technologie de l'information, qui peuvent être impliqués dans leur mise en œuvre.

Annexe à la Recommandation n° R (95) 13

relative aux problèmes de procédure pénale liés à la technologie de l'information

I. Perquisition et saisie

1. La distinction opérée par le droit entre la perquisition de systèmes informatiques ainsi que la saisie des données qu'ils renferment et l'interception de données au cours de la transmission devrait être clairement délimitée et appliquée.

2. Les lois de procédure pénale devraient permettre aux autorités chargées de l'enquête de perquisitionner dans les systèmes informatiques et d'y saisir des données, dans des conditions similaires à celles utilisées dans le cadre des pouvoirs traditionnels de perquisition et de saisie. La personne en charge du système devrait être informée que le système a fait l'objet d'une perquisition et de la nature des données saisies. Les recours juridiques prévus par la législation en général contre la perquisition et la saisie devraient être également applicables en cas de perquisition d'un système informatique et de saisie des données qui y sont contenues.

3. Durant l'exécution de la perquisition, les autorités chargées de l'enquête devraient avoir le pouvoir, sous réserve de garanties appropriées, d'étendre la perquisition à d'autres systèmes informatiques dans leur juridiction qui sont connectés par le biais d'un réseau et d'y saisir des données, à condition qu'une action immédiate soit requise.

4. S'il y a équivalence fonctionnelle entre les données faisant l'objet de traitement automatisé et un document traditionnel, les dispositions du droit de procédure pénale se rapportant aux documents devraient également s'appliquer aux données.

II. Surveillance technique

5. Etant donnée la convergence de la technologie de l'information et des télécommunications, les législations concernant la surveillance technique employée à des fins d'enquêtes pénales, comme l'interception des communications, devraient être, là où cela s'avère nécessaire, révisées et amendées pour assurer leur applicabilité.

6. La loi devrait permettre aux autorités chargées de l'enquête d'appliquer toute mesure technique permettant la collecte de données de trafic dans la poursuite des infractions pénales.

7. Lorsqu'elles sont collectées au cours d'une enquête pénale et en particulier quand elles sont obtenues par des moyens d'interception des télécommunications, les données protégées par la loi et faisant l'objet du traitement automatisé par un système informatique devraient être sauvegardées de manière appropriée.

8. Les lois de procédure pénale devraient être révisées en vue de rendre possible l'interception de télécommunications et la collecte de données de trafic dans le cadre d'enquêtes sur des infractions graves contre la confidentialité, l'intégrité et la disponibilité des systèmes de télécommunications ou informatiques.

III. Obligations de coopération avec les autorités chargées de l'enquête

9. Sous la réserve des protections ou privilèges prévus par la loi, la plupart des législations permettent aux autorités chargées de l'enquête d'ordonner à des personnes de remettre des objets qui sont sous leur contrôle et qui sont

requis pour servir de preuve. Le droit de procédure pénale devrait, de la même manière, accorder le pouvoir d'ordonner à des personnes de leur présenter toute donnée spécifique qui se trouve sous leur contrôle, dans un système informatique, dans la forme requise par les autorités chargées de l'enquête.

10. Sous la réserve des protections ou privilèges prévus par la loi, les autorités chargées de l'enquête devraient avoir le pouvoir d'ordonner aux personnes qui ont des données spécifiques sous leur contrôle de fournir toutes les informations nécessaires pour permettre l'accès au système informatique et aux données qu'il renferme. Le droit de procédure pénale devrait assurer que les autorités chargées de l'enquête puissent donner une instruction similaire à d'autres personnes ayant une connaissance du fonctionnement du système informatique ou de toute mesure employée pour préserver les données y contenues.

11. Des obligations spécifiques devraient être établies pour les opérateurs de réseaux publics et de réseaux privés, lorsqu'ils offrent des services de télécommunication au public, d'appliquer toute mesure technique nécessaire permettant l'interception des télécommunications par les autorités chargées de l'enquête.

12. Des obligations spécifiques devraient être établies pour les fournisseurs de services qui offrent des services de télécommunication au public via des réseaux de communication publics ou privés, de délivrer l'information nécessaire, lorsque les autorités compétentes chargées de l'enquête l'ordonnent, pour identifier l'utilisateur.

IV. La preuve électronique

13. L'intérêt commun de recueillir, de sauvegarder et de présenter des preuves électroniques de manière à garantir au mieux leur caractère irréfutable et leur intégrité devrait être reconnu tant pour les fins des poursuites nationales que pour celles de la coopération internationale. A cette fin, des procédures et méthodes techniques du traitement des preuves électroniques devraient être développées davantage de manière à assurer leur compatibilité entre les Etats. Les dispositions du droit de procédure pénale concernant les preuves et se rapportant aux documents traditionnels devraient également s'appliquer aux données stockées dans un système informatique.

V. Utilisation du chiffrement

14. Des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale.

VI. Recherche, statistiques et formation

15. Le risque qu'impliquent le développement et l'utilisation de la technologie de l'information sur la perpétration des infractions pénales devrait faire l'objet d'une évaluation continue. Afin de permettre aux autorités compétentes de rester familiarisées avec de nouveaux phénomènes en matière de criminalité informatique et de pouvoir développer des contre-mesures adéquates, la collecte et l'analyse des données concernant ces infractions, y compris le *modus operandi* et les aspects techniques, devraient être favorisées.

16. La création d'unités spécialisées pour la répression d'infractions dont la poursuite requiert une expérience spéciale en matière de technologie de l'information devrait être examinée. Des programmes de formation permettant au personnel de la justice pénale d'approfondir leurs connaissances en la matière devrait être promus.

VII. Coopération internationale

17. Le pouvoir d'étendre la perquisition à d'autres systèmes informatiques devrait être également applicable lorsque le système se trouve sous une juridiction étrangère, à condition qu'une action immédiate soit requise. En vue d'éviter d'éventuelles violations de la souveraineté des Etats ou du droit international, une base légale explicite devrait être créée pour de telles perquisitions ou saisies étendues. Par conséquent, il y a un besoin urgent de négocier des instruments internationaux quant à la question de savoir comment, quand et dans quelle mesure de telles perquisitions ou saisies peuvent être permises.

18. Des procédures accélérées et appropriées ainsi qu'un système de liaison devraient être disponibles selon lesquels les autorités chargées de l'enquête pourraient demander aux autorités étrangères de recueillir promptement des preuves. A cette fin, les autorités requises devraient être autorisées à perquisitionner dans un système informatique et à y saisir des données en vue de leur transfert ultérieur. Les autorités requises devraient également être autorisées à délivrer des données de trafic se rapportant à une télécommunication spécifique, à intercepter une telle télécommunication ou à identifier sa source. A cette fin, les instruments d'entraide judiciaire existants devraient être complétés.