

N° 6763⁴

CHAMBRE DES DEPUTES

Session ordinaire 2014-2015

PROJET DE LOI

portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

* * *

SOMMAIRE:

	<i>page</i>
1) Dépêche du Procureur Général d'Etat au Ministre de la Justice (28.7.2015).....	1
2) Avis de la Cour Supérieure de Justice (19.2.2015).....	2
3) Avis du cabinet d'instruction de Luxembourg (19.2.2015)	4
4) Avis du Parquet de Luxembourg	
– Dépêche du Procureur d'Etat de Luxembourg au Procureur Général d'Etat (3.2.2015)	5
5) Avis du Parquet de Diekirch (13.2.2015).....	6
6) Avis du Parquet Général (29.7.2015)	8

*

**DEPECHE DU PROCUREUR GENERAL D'ETAT
AU MINISTRE DE LA JUSTICE**

(28.7.2015)

Monsieur le Ministre,

Le 5 janvier 2015 vous avez fait parvenir au soussigné le projet de loi sous rubrique avec prière de solliciter également les avis de la Cour Supérieure de Justice, des parquets et des cabinets d'instruction de Luxembourg et de Diekirch.

A ce jour les avis suivants ont été transmis au Parquet général

- l'avis de la Cour Supérieure de Justice
- l'avis de Monsieur le juge d'instruction directeur du Luxembourg
- l'avis de Monsieur le procureur d'Etat de Luxembourg
- l'avis de Monsieur le procureur d'Etat de Diekirch

Ces documents sont joints à la présente de même que l'avis du soussigné de ce jour.

Le Procureur Général d'Etat,
Robert BIEVER

*

AVIS DE LA COUR SUPERIEURE DE JUSTICE

(19.2.2015)

Le projet de loi tend à modifier l'article 67-1, alinéa 1er, du code d'instruction criminelle relatif aux écoutes judiciaires à ordonner par le juge d'instruction saisi de faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, en remplaçant cette désignation générale des infractions permettant le recours aux écoutes judiciaires, par une énumération détaillée et limitative des différentes infractions pouvant entrer en ligne de compte et devant figurer dorénavant dans un nouvel alinéa 4.

La liste des infractions graves proposée dans le projet de loi est inspirée par l'annexe D de la directive 2014/41/CE du Parlement Européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale.

L'établissement d'une liste exhaustive des infractions serait exigée par l'arrêt rendu le 8 avril 2014 par la Cour de Justice de l'Union Européenne (CJUE) dans les affaires jointes C-293/12 et C-594/12, par lequel la Cour a invalidé la directive 2006/24/CE du Parlement Européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications.

L'arrêt du 8 avril 2014 de la CJUE a invalidé la directive 2006/24/CE notamment parce qu'elle ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, entre autres en ce qu'elle se borne à renvoyer, à son article 1er, § 1, de manière générale aux infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne (n° 60 de l'arrêt).

Il faut cependant se garder d'en induire que la directive 2006/24/CE serait pour ce seul motif contraire aux droits garantis par la Charte. Ce résultat s'explique par un ensemble de déficiences exposées par la CJUE qui l'ont amenée à conclure à une violation du principe de proportionnalité au regard des articles 7, 8, et 52, § 1, de la Charte.

Le progrès censé être procuré par l'établissement d'une liste limitative des infractions qualifiées de graves n'est pas évident, la gravité d'une infraction se définissant toujours par la rigueur de la peine d'emprisonnement comminée.

La durée minimum de la peine d'emprisonnement qui doit être encourue pour permettre le recours aux écoutes judiciaires varie d'un pays à l'autre. Au Luxembourg une peine d'emprisonnement d'au moins un an est suffisante, tandis qu'en France, l'article 100 du code de procédure pénale exige une peine égale ou supérieure à deux ans d'emprisonnement.

La confection d'une liste n'est pas de nature à contribuer à une harmonisation plus poussée sur le plan européen. L'article 90ter, § 2, du code d'instruction criminelle belge comporte une énumération des infractions pouvant justifier une mesure de surveillance partiellement différente de celle prévue par le projet de loi.

Cette harmonisation n'est d'ailleurs nullement requise, puisque la mesure de surveillance de l'article 67-1 du code d'instruction criminelle a un champ d'application territorial ou national et non européen. Chaque Etat définit comme il l'entend les infractions graves qui justifient une surveillance des télécommunications sur son territoire. Il n'existe donc en l'état actuel du droit communautaire aucune nécessité, voire obligation, de recourir à une soi-disant liste européenne des infractions graves.

La liste des infractions graves proposée dans le projet de loi constitue une énumération pêle-mêle de délits et de crimes repris, sans aucun ordre ni logique de classification apparente, tantôt du code pénal tantôt de lois spéciales. Il faut en outre constater que la liste proposée comporte des lacunes, ce qui est un désavantage inhérent à la méthode choisie, et que l'énumération manque de cohérence (voir par exemple le n° 24 relatif au vol) et les indications relatives aux infractions sont dans plusieurs cas partiellement contradictoires en ce sens que les infractions nommément visées ne correspondent pas exactement avec les articles du code pénal auxquels il est fait référence.

Ainsi à titre d'exemples:

Quant au **n° 1) crimes et délits contre la sûreté de l'Etat** (articles 101 à 123 du code pénal).

L'intitulé vise les „crimes et délits contre la sûreté de l'Etat“ sans distinction entre la sûreté extérieure et la sûreté intérieure de l'Etat. Les articles mentionnés ne concernent cependant que les infractions à

la sûreté extérieure de l'Etat. Qu'en est-il des articles 124 à 135 du code pénal? Qu'est ce qui doit l'emporter: les infractions visées par les articles indiqués ou les infractions comprises dans la désignation générale „crimes et délits contre la sûreté de l'Etat“?

Dans d'autres cas, c'est l'inverse: les articles du code pénal mentionnés vont au-delà de l'infraction nommément indiquée (par exemple le n° 28 relatif au faux).

Quant au **n° 8fraudes et abus de confiance (articles 489 à 509 du code pénal), y compris la fraude portant sur l'atteinte aux intérêts financiers des Communautés Européennes (...).**

Le terme „fraude“ est un terme générique qui englobe plusieurs infractions spécifiques, comme, entre autres, l'abus de confiance, mais aussi la banqueroute (frauduleuse), l'abus de faiblesse et l'escroquerie.

Soit on énumère toutes les infractions spécifiques rentrant dans la notion de „fraude“ et non seulement l'une d'elle, en l'occurrence l'abus de confiance, soit on se borne à indiquer une notion générale („fraudes“) et les articles du code pénal y relatifs sans autre précision.

Mais on ne peut pas, sans créer une équivoque, mentionner seulement l'abus de confiance et pour le surplus se référer les articles 489 à 509 du code pénal. On se demande ce qui doit l'emporter, l'énoncé de l'infraction ou les articles du code pénal?

On s'interroge en outre pourquoi l'escroquerie, qui constitue un cas de fraude comme l'abus de confiance, figure à part, au **n° 26**.

A remarquer que l'infraction d'abus de biens sociaux ne figure pas sur la liste.

Quant au **n° 12blanchiment des produits du crime et recel (articles 505 à 506-8 et 508 à 509 du code pénal), le blanchiment et le recel sont nommément mentionnés, mais pas le cel et les traites de complaisance bien que les articles qui les concernent le soient.**

Quant au **n° 24vol commis à l'aide de violences ou menaces et extorsion (articles 468 à 476 du code pénal).**

La liste contient encore un **n° 31consacré au vol commis sans violences ni menaces (articles 463 à 467 du code pénal) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.**

Qu'en est-il du vol simple et du vol qualifié (avec effraction, escalade ou fausses clefs, vol commis par fonctionnaire public à l'aide de ses fonctions, par des voleurs qui ont pris le titre ou les insignes d'un fonctionnaire public ou qui ont allégué un faux ordre de l'autorité publique article 467 code pénal) sans lien avec une association de malfaiteurs ou une organisation criminelle?

Pourquoi ne pas regrouper tous les cas de vol sous un seul numéro?

Pourquoi intégrer un délit mineur comme le cel dans la liste des infractions graves et en écarter des crimes comme les vols qualifiés visés à l'article 467 du code pénal, non commis dans le cadre d'une association de malfaiteurs?

Pourquoi retenir spécialement le vol commis sans violences ni menaces (articles 463 à 467 du code pénal) dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle bien que la simple participation à une association de malfaiteurs ou à une organisation criminelle permette déjà une surveillance judiciaire indépendamment de tout vol (n° 2 de la liste)?

Les infractions de contrefaçon visées aux articles 179 à 191 du code pénal (**n° 27**) devraient figurer logiquement avec le faux-monnayage (n° 13).

Quant au **n° 28qui vise la falsification de documents administratifs et usage de faux ensemble avec les articles 193 à 212 du code pénal.**

Pourquoi mentionner nommément la „falsification de documents administratifs“, notion qui ne figure pas au code pénal, alors que les articles 193 à 212 traitent du faux en écritures authentiques et publiques, en écritures de commerce ou de banque et en écritures privées ainsi que du faux commis dans les passeports, permis de chasse ou de pêche, livrets, feuilles de route, certificats et attestations?

On remarque au passage, à titre d'exemple, que ni l'infraction de faux bilan ni les infractions de faux témoignage, de faux serment et de subornation ne figurent dans la liste des infractions graves,

bien que, par exemple, le faux témoignage en matière criminelle soit puni de la réclusion de cinq à dix ans.

Il en est de même du crime prévu à l'article 235 du code pénal qui n'est pas visé au n° 1 de la liste qui se réfère uniquement aux articles 101 à 123 du code pénal.

Il serait peut-être préférable de maintenir en l'état actuel des choses l'article 67-1 dans sa version actuelle.

Subsidiairement, si l'on veut néanmoins établir une liste des infractions graves, il serait avantageux de suivre l'ordre des infractions dans le code pénal et indiquer ensuite les infractions prévues dans les lois spéciales entrant en ligne de compte.

*

AVIS DU CABINET D'INSTRUCTION DE LUXEMBOURG

(19.2.2015)

Le projet de loi a pour but d'adapter notre législation suite à l'arrêt rendu par la Cour de Justice de l'Union Européenne en date du 8 avril 2014, qui a invalidé la directive 2006/12/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de détection et de poursuite des infractions graves.

La directive invalidée avait été transposée par la loi du 30 mai 2005 qui a retenu une durée de conservation des données de seulement 6 mois, tout en adoptant un critère assez large pour déterminer l'infraction grave justifiant ainsi l'accès aux données qui était donné à chaque fois qu'une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement était prévue.

L'article 67-1 du code d'instruction criminelle tel qu'introduit par une loi du 21 novembre 2002 réserve le repérage téléphonique au seul juge d'instruction, délimite son champ d'application des données avec l'obligation pour le magistrat d'indiquer dans une ordonnance motivée qu'il communique au procureur d'Etat les circonstances de fait de la cause justifiant la mesure.

Le projet de loi sous discussion maintient le principe de la conservation des données de télécommunications pendant un délai de 6 mois au plus et se propose de définir de manière limitative et exhaustive les infractions graves par une énumération de 33 catégories d'infractions reprise de l'article 11 de la directive 2014/41/UE.

L'idée du projet de loi est d'énumérer dans le paragraphe 4 nouveau de l'article 67-1 du Code d'Instruction criminelle des catégories d'infractions pour lesquelles les autorités répressives peuvent avoir accès aux données de communications obtenues. Cette liste s'inspire de la liste des infractions prévues à l'annexe D de la directive 2014/41/UE du parlement européen et du conseil du 3 avril 2014 concernant la décision d'enquête européennes en matière pénale. Cette liste a été dressée pour une finalité qui s'apparente, dans le contexte de l'entraide pénale internationale, à celle du recours aux données de communications retenues par les opérateurs de télécommunications. Le projet propose cependant d'amender cette liste en la précisant par des renvois à des articles déterminés du Code pénal et de certaines lois spéciales afin de l'adapter aux spécificités du droit pénal luxembourgeois.

Force est de constater qu'une nouvelle liste d'infractions à ajouter dans notre législation pénale nationale aura nécessairement comme conséquence que les règles de procédure pénale deviennent de moins en moins lisibles et que leur application devient de plus en plus difficile pour les praticiens et à la limite incompréhensible pour les justiciables.

Le projet de loi abandonne d'une certaine manière le principe de la sécurité juridique assurée sur le critère objectif du seuil de peine privative de liberté dont le maximum est égal ou supérieur à 1 an en adoptant une nouvelle liste d'infractions qui s'inspirent de notions et de concepts repris d'une directive UE en y ajoutant des articles déterminés du Code pénal luxembourgeois et de certaines lois spéciales.

La liste des infractions figurant dans le projet de loi sous examen appelle les observations suivantes:

- a) Il convient de relever d'emblée que ne figurent pas dans la liste certains délits et notamment la fausse alerte et la menace d'attentat alors que ces infractions sont très souvent perpétrées par l'utilisation de communication téléphoniques ou électroniques et que très souvent aussi le seul moyen

afin de pouvoir les élucider consistant à faire procéder du moins dans un premier temps à un retraçage de ces communications.

- b) Il convient aussi de s'interroger à la lecture de la liste des infractions sur la notion du trafic qui est une notion et un concept repris du droit international et qui n'existe pas comme infraction spécifique dans le droit pénal luxembourgeois.
- c) Force est également de relever que certaines infractions n'atteignent pas le degré de gravité requis afin de justifier le retraçage et le repérage de télécommunications que si elles ont été commises dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle alors que d'autres infractions sont considérées comme suffisamment graves sans cette circonstance aggravante comme en espèce le recel (point 12 de la liste des infractions). Il convient par ailleurs de souligner que le vol simple repris dans le point 31 dans la même liste exige pour justifier la mesure de repérage que ce dernier a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Le juge d'instruction directeur,
Ernest NILLES

*

AVIS DU PARQUET DE LUXEMBOURG

DEPECHE DU PROCUREUR D'ETAT DE LUXEMBOURG AU PROCUREUR GENERAL D'ETAT

(3.2.2015)

Monsieur le Procureur Général d'Etat,

Comme suite à votre demande du 16 janvier 2015, je me permets de vous soumettre l'avis du Parquet de Luxembourg sur le projet de loi visé.

Le texte en projet entend mettre la législation pénale luxembourgeoise en adéquation avec l'arrêt de la Cour de Justice de l'Union Européenne, pour autant que cela soit possible.

L'opportunité de la démarche n'est donc pas à discuter. Les dispositions en projet, pour ne pas abandonner de manière intégrale la possibilité de recourir à l'exploitation des données de télécommunications pour les besoins de l'instruction de certaines infractions, visent donc principalement et en premier lieu à remplacer la référence à un certain seuil de peine privative de liberté pour déterminer les infractions entrant en ligne de compte, par une liste d'infractions nommément désignées. Une liste comporte des risques d'omission et le recours à cette méthode a déjà fait l'objet de critiques à de nombreuses reprises dans le cadre de l'examen d'autres textes de loi dans le domaine pénal et de procédure pénale.

Il convient donc d'apprécier si les dispositions arrêtées par le Projet de loi sont en concordance avec les réalités de la lutte contre la criminalité.

A cet égard le commentaire se limitera à révéler certaines lacunes dans la liste et à proposer en conséquence certaines adjonctions et certaines modifications/rectifications.

Ad article 1er – PL 6763

Il convient de compléter la liste développée sous 2) de l'article 1er du Projet de loi, par l'infraction de fausse alerte – article 319 CP, de même que par celle des menaces d'attentat – article 327 CP et celle des offres ou propositions de commettre un crime – article 331 CP, infractions qui souvent comportent le recours à des moyens de télécommunication.

Au point 7) de la même liste, aux fins d'être complet dans le domaine des infractions de corruption et apparentées, il convient d'ajouter l'infraction de prise illégale d'intérêts et d'indiquer en début de la référence aux articles du Code pénal visés, l'article 245 CP.

Au point 8) de la même liste, aux fins d'être complet dans le domaine des comportements frauduleux, il convient d'ajouter l'infraction d'abus de biens sociaux (article 171-1 de la loi modifiée du 10 août 1915 concernant les sociétés commerciales).

Au point 13) de la liste, il est préférable de remplacer les termes „faux monnayage et contrefaçon de monnaie“ par les termes „contrefaçon de moyens de paiement, de titres, de sceaux, timbres, poinçons, marques. etc.“ les articles du Code pénal indiqués entre parenthèses couvrant des hypothèses diverses allant bien au-delà de la fausse monnaie.

Au point 27) de la liste, il convient de préciser qu’est visée la contrefaçon „d’œuvres protégées par des droits de propriété intellectuelle (Loi modifiée du 18 avril 2001 sur les droits d’auteur, les droits voisins et les bases de données)“, les articles 179 à 191 du Code pénal se trouvant déjà repris sous le point 13) de la liste.

Au point 28) de la liste il est préférable de remplacer les termes „falsification de documents administratifs“ par le terme „faux“, en raison des termes „usage de faux“ employés par la suite et au regard des infractions visées par les articles du Code pénal indiqués entre parenthèses; dans le même contexte il convient de remplacer l’article 212 par 214, plus adapté.

Au point 31) de la liste, il convient de faire abstraction du cadre spécifique visé pour l’infraction de vol sans violence ni menaces, les autres infractions contre la propriété, comme les fraudes et abus de confiance et l’escroquerie, de même que le recel, n’étant pas non plus limitées par la condition de devoir se situer dans le cadre des agissements d’une association ou organisation criminelle.

L’article 2 du Projet de loi ne soulève pas d’observations particulières.

Profond respect.

Le Procureur d’Etat,
J.P. FRISING

*

AVIS DU PARQUET DE DIEKIRCH

(13.2.2015)

Le projet de loi a pour but d’adapter notre législation suite à l’arrêt rendu par la Cour de Justice de l’Union Européenne en date du 8 avril 2014, qui a invalidé la directive 2006/12/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.

La Cour a plus particulièrement reproché à cette directive d’avoir omis de prévoir des règles claires et précises en vue de régir la portée de l’ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, constatant que la directive comportait une ingérence d’une vaste ampleur dans ces droits fondamentaux et d’une gravité particulière dans l’ordre juridique de l’Union, sans que cette ingérence fût précisément encadrée par des dispositions permettant de garantir qu’elle se limitait effectivement au strict nécessaire. (cf. Arrêt pt. 65)

La Cour a ainsi critiqué:

- a. L’absence générale de limite (Arrêt pt. 58 et 59)
 - o La directive visait de manière globale toute personne faisant usage de services de communications électroniques (peu importe l’existence d’indices d’infraction ou le secret professionnel).
 - o La directive n’exigeait aucune relation entre les données dont la conservation était prévue et une menace pour la sécurité publique (période temporelle, zone géographique, cercle de personnes suspectées).
- b. L’absence de critère objectif pour délimiter l’accès des autorités nationales compétentes et leur utilisation ultérieure (Arrêt pt. 60 à 62).
- c. S’agissant de la durée de conservation des données, la directive fixait un délai sans que fût opérée une distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l’objectif poursuivi ou selon les personnes concernées. La durée de conservation (entre 6 et 24 mois) aurait dû être fondée sur des critères objectifs afin de garantir que celle-ci fut limitée au strict nécessaire (Arrêt pt. 63 et 64).
- d. La protection des données par les fournisseurs accompagnée de l’obligation de destruction irrémédiable au terme de la durée de conservation et de conservation sur le territoire de l’Union, n’était pas suffisamment garantie (p. 66 et 67).

La directive invalidée avait été transposée par la loi du 30 mai 2005 qui opta pour une durée de conservation des données très courte (6 mois), tout en adoptant un critère assez large pour déterminer l'infraction grave, et justifiant ainsi l'accès aux données, qui était donné chaque fois qu'une peine correctionnelle d'un maximum égal ou supérieur à un emprisonnement d'un an était prévue par la loi.

Le projet de loi sous discussion maintient le principe de la conservation des données de télécommunication pendant un délai de 6 mois au plus, ce qui fut le minimum prévu par la directive invalidée, et se propose de définir restrictivement et limitativement les infractions graves par une énumération de 33 infractions qui est reprise de l'article 11 de la directive 2014/41/UE.

L'article 11 de cette directive énonce les motifs possibles d'une non-reconnaissance ou non-exécution d'une décision d'enquête européenne, c'est-à-dire les cas où un Etat dispose de la faculté de refuser la reconnaissance ou l'exécution d'une décision d'enquête européenne. Conformément à l'article 11, point g), cette faculté est exclue au cas où les faits constituent dans l'Etat d'émission une des susdites 33 infractions et sont punissables dans le pays d'émission d'une peine ou d'une mesure de sûreté privative de liberté d'un maximum d'au moins trois ans.

Le fait d'ajouter une nouvelle liste d'infractions dans notre législation pénale nationale, en dehors de celles qui y figurent d'ores et déjà comme par exemple celle prévue dans la loi sur le mandat d'arrêt européen (loi modifiée du 17 mars 2004, article 3) ou celle inscrite à l'article 506-1 du Code pénal sur l'infraction de blanchiment, aura non seulement comme conséquence inéluctable que les règles de procédure pénale deviendront de moins en moins lisibles, mais également que leur application deviendra de plus en plus difficile pour les praticiens, voire incompréhensible pour les justiciables.

Au lieu de veiller à créer des règles de procédure pénale claires et facilement prévisibles pour toute personne visée par une instruction ou pour toute victime préjudiciée par une telle infraction, on aboutira de plus en plus à faire application de textes compliqués, avec des listes d'infractions variables, sans relation apparente avec la gravité des peines prévues par le législateur.

Si on peut comprendre l'initiative du législateur d'énumérer les infractions qui, à ses yeux, relèvent d'une gravité telle que leur élucidation devrait pouvoir se faire, dans des circonstances spécialement motivées par un juge d'instruction, en procédant par un repérage et retraçage de télécommunications et de ne plus maintenir le seuil fixé par la loi du 30 mai 2005 à une peine d'emprisonnement correctionnel d'un maximum égal ou supérieur à un an pour définir cette gravité, il est par contre difficilement compréhensible pourquoi tous les crimes, infractions punissables d'une peine de réclusion, partant d'une peine particulièrement grave et sévère aux yeux du législateur, ne seraient pas considérés comme suffisamment graves pour justifier, dans les mêmes circonstances spéciales dûment motivées, le recours au retraçage et au repérage de télécommunications pour les élucider.

Il est dès lors proposé d'ajouter à la liste, à l'instar de ce qui a été fait en matière de blanchiment, **„ainsi que toute autre infraction punie d'une peine criminelle“**.

Comment peut-il en effet se justifier qu'en matière de crime, certaines mesures d'investigation seraient exclues d'emblée par le législateur, nonobstant les circonstances exceptionnelles d'une espèce déterminée à relever par le juge d'instruction, et à contraindre les organes de poursuite à se résigner, dans ces hypothèses, à ne pas pouvoir utiliser toutes les mesures techniques disponibles pour essayer de les élucider.

La liste d'infractions figurant actuellement dans le projet de loi, appelle de surcroît les observations suivantes:

- a. Il est étonnant de constater que dans un texte à vocation nationale, le législateur entend faire figurer des notions et concepts repris d'une directive UE, mais n'existant pas en tant que tels en droit luxembourgeois, telle que la notion de „trafic“, et il est difficile de voir l'utilité de recourir en droit national à ces concepts de droit international.
- b. En termes de technique législative, il semble également surprenant de se référer principalement des incriminations reprises d'une directive UE pour les faire correspondre en quelque sorte en ordre subsidiaire, puisque énoncées entre parenthèses, à des infractions prévues dans notre législation nationale, alors qu'il pourrait sembler plus adéquat de faire principalement référence à des infractions prévues dans notre législation nationale, avec des éléments constitutifs bien définis et facilement déterminables, avant de se référer à des notions internationales qui ont essentiellement vocation à englober toutes les spécificités des différentes législations des Etats membres.

Ainsi, à titre d'exemple, il convient de renvoyer à l'infraction visée au point 28) „falsification de documents administratifs et usage de faux (art. 193 à 212 du Code pénal)“, puisque la législation

nationale énoncée entre parenthèses vise la perpétration de faux commis en écritures tant publiques que privées ainsi que l'usage de ces faux, et ne se limite nullement à une falsification de documents administratifs.

- c. Il paraît encore discutable qu'un certain nombre d'infractions n'atteignent le degré de gravité requis pour justifier le repérage et le retraçage de télécommunications que si elles ont été commises „dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle“ (points 18, 20, 29, 30 et 31), alors que d'autres sont considérées comme assez graves sans cette circonstance aggravante, dont par exemple le recel prévu au point 12. Or, le vol simple mentionné au point 31, lequel peut être à la base du recel, n'y figure que dans l'hypothèse où il a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Il convient d'y ajouter la grivèlerie (peine maximale 6 mois d'emprisonnement au vu de l'article 491 du Code pénal), les coups et blessures simples (peine maximale 6 mois d'emprisonnement maximum au vu de l'article 398 du Code pénal) qui sont, d'après le projet de loi, per se d'une gravité telle qu'elles peuvent justifier l'accès aux données de communication, alors qu'au vu du point 31 un vol à l'aide d'effraction ou de fausse clé (article 467 du Code pénal) n'est considéré comme infraction assez grave pour justifier cette mesure que s'il a été commis dans le cadre d'une association de malfaiteurs ou d'une organisation criminelle.

Le Code pénal met d'ailleurs sur le même pied en termes de peines et donc de gravité (réclusion de 5 à 10 ans) le vol qualifié de l'article 467 (point 31) avec celui commis à l'aide de violences ou de menaces de l'article 468 du Code pénal (point 24), ce dernier n'ayant toutefois pas besoin d'être commis dans le cadre d'une association de malfaiteurs pour permettre un repérage des télécommunications.

- d. Reste à relever que les délits de fausse alerte et de menaces d'attentat ne figurent pas dans la liste, malgré le fait que ceux-ci sont très souvent perpétrés par le biais de communications téléphoniques ou électroniques, et que ces délits ne peuvent ainsi être élucidés dans la majorité des cas que par un retraçage de ces communications.

*Le Procureur d'Etat près le Tribunal
d'arrondissement de Diekirch,*

Aloyse WEIRICH

*

AVIS DU PARQUET GENERAL

(29.7.2015)

I) REMARQUE PRELIMINAIRE

Aux termes de l'exposé des motifs le projet de loi tend à „adapter le dispositif légal relatif à la rétention des données de télécommunications à des fins de poursuites pénales aux exigences de l'arrêt rendu par la Cour de Justice de l'Union européenne en date du 8 avril 2014, dit „Digital Rights“ (affaires jointes C-293/12/ et C-594/12), par lequel la Cour a invalidé la directive 2006/24/CE du 15 mars 2006 relative à la conservation de données à caractère personnel à des fins de prévention, de recherche, de détection et de poursuite des infractions graves.“.

Le projet tend donc à modifier notre législation pour l'adapter suite à l'arrêt de la Cour de Justice de l'Union européenne invalidant la directive 2006/24/CE du 15 mars 2006 relative à l'objet indiqué ci-avant.

Il se trouve toutefois que notre loi, qui date du 30 mai 2005, n'a pas transposé en droit luxembourgeois la directive 2006/24¹.

Il s'y ajoute que lors de la modification de la loi du 30 mai 2005 par la loi du 18 juillet 2011, on n'a pas fait la moindre référence à la directive 2006/24 qui allait être annulée le 8 avril 2014.

¹ Il ne s'agit en l'occurrence en rien d'une simple erreur matérielle de dates.

A préciser que ni dans les travaux parlementaires ayant abouti à la loi de 2005 ni dans ceux qui ont abouti à la loi de 2011 il n'est fait la moindre référence à la directive (annulée) 2006/24.

Notre législation est donc tout à fait indépendante des dispositions du droit de l'Union Européenne, qui ont été invalidées par l'arrêt „Digital Rights“.

Il en résulte, et le point est important voire essentiel, que l'annulation de la directive visée par la Cour de Justice de l'Union Européenne n'a aucune incidence sur la validité de la législation luxembourgeoise et ce d'autant moins que dans sa motivation la Cour de Justice de l'Union Européenne s'est uniquement basée sur des articles relatifs à la protection de la vie privée figurant dans la Charte des droits fondamentaux de l'Union Européenne. Or, cette Charte dispose dans son article 51, paragraphe 1, que ses dispositions „s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres uniquement lorsqu'elles mettent en oeuvre le droit de l'Union.“.

La loi luxembourgeoise modifiée de 2005 n'ayant pas mis en oeuvre le droit de l'Union Européenne, l'arrêt de la Cour de Justice de l'Union Européenne n'a juridiquement aucune incidence sur la validité de notre législation².

*

L'avis relatif au projet soumis pourrait dès lors parfaitement s'arrêter ici.

Toutefois l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (C.E.D.H.) protège également la vie privée des citoyens et n'admet des exceptions à ce principe que si celles-ci sont proportionnelles à l'atteinte à la vie privée et justifiées notamment par la sûreté et la sécurité.

La C.E.D.H. étant d'application directe elle peut être invoquée directement devant nos juridictions.

Dès lors, qu'on le veuille ou non, la question risque de surgir sous peu sous une forme ou une autre devant nos juridictions ou encore devant le Cour Européenne des Droits de l'Homme elle-même et il

2 La Belgique avait transposé la directive 2006/24/CE (invalidée par l'arrêt C-293/12 et C-594/12 de la CJUE du 8 avril 2014) par une loi du 30 juillet 2013. Cette loi avait notamment modifié par son article 5 un article 126 d'une loi du 13 juin 2005 relative aux communications électroniques en faisant précisément et de manière expresse référence à la directive 2006/24. Sans le cadre d'un recours devant la Cour constitutionnelle de Belgique les requérants ont considéré que la loi de 2013, et notamment son article 5, méconnaissent l'arrêt de la CJUE.

La thèse du Gouvernement belge était de soutenir:

- o Que certes l'arrêt de la CJUE a pour effet d'obliger tout juge de considérer la directive comme invalide.
- o Que ce constat s'étend aux dispositions nationales qui transposent la directive. Ces dispositions perdent leur validité par suite de l'arrêt de la Cour (A.5.1.).
- o Que ce ne seraient cependant que les articles 2 et 3 de la loi de 2013 auxquels s'appliquerait ce sort.
- o Qu'en revanche l'article 5 de la loi pourrait être séparé du reste de la loi attaquée, de sorte que l'irrégularité d'autres articles de cette loi n'affecterait pas l'article 5 (A.5.1.).
- o Que l'arrêt de la CJUE, en invalidant la directive, redonne compétence aux Etats membres de régler la problématique de la rétention des données (faute d'harmonisation en la matière) (idem).
- o Que l'article 5 de la loi n'est donc doublement pas affectée par l'arrêt: il ne transposerait pas la directive, donc ne tomberait pas avec celle-ci et il s'appliquerait, suite à l'invalidation de la directive, dans un domaine dans lequel le législateur belge reste libre de légiférer sans interférence du droit de l'Union européenne. (A.5.1 et B.7).

La Cour constitutionnelle de la Belgique a par un arrêt du 11 juin 2015 rejeté ce raisonnement au motif, en substance, que l'article 5 transpose bien la directive, donc tombe avec elle et se voit, dans la mesure où il transpose la directive, appliquer la Charte des droits fondamentaux (B.8).

La Charte des droits fondamentaux dispose dans son article 51, paragraphe 1, que ses dispositions „s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres **uniquement lorsqu'ils mettent en oeuvre le droit de l'Union**“.

Tel ayant été le cas en Belgique la Cour constitutionnelle du Royaume de Belgique a, par l'arrêt du 11 juin 2015 annulé la loi belge afférent qui a été adoptée précisant en vue de mettre en oeuvre le droit de l'Union Européenne.

La Cour constitutionnelle note dans son arrêt que les méthodes proposées par les requérants pour séparer les métadonnées des avocats de celles du commun des mortels sont impraticables (voir notamment A.3.3.). La seule issue possible serait de renoncer à la rétention de données. C'est le tout ou rien. Voir le point A.4.5, résumant la thèse des requérants: „Quant à l'impossibilité invoquée de mettre en oeuvre une distinction selon que les données émanent de titulaires du secret professionnel ou d'autres personnes, ces difficultés ne justifieraient pas qu'une annulation pure et simple de la disposition critiquée ne puisse être prononcée afin de mettre fin à une situation discriminatoire“.

est à prévoir que les requérants soulèveront alors plus ou moins les mêmes moyens que ceux qui ont été abordés dans l'arrêt de la Cour de Justice de l'Union Européenne du 8 avril 2014.

Il est dès lors indispensable d'analyser le problème.

*

**II) ANALYSE SUCCINCTE DE L'ARRET DE LA COUR DE
JUSTICE DE L'UNION EUROPEENNE
du 8 avril 2014 par lequel la directive 2006/24 de l'Union Européenne
a été annulée, l'arrêt peut être résumé comme suit:**

La Cour de Justice de l'Union européenne a annulé la directive 2006/24/CE (ci-après la directive) après un examen approfondi des textes aux motifs notamment que „*cette directive importe une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire*“ (point 65), après avoir relevé que, **les dispositions de la directive 2006/24/CE relative à la conservation des données électroniques portent atteinte à certaines dispositions de la Charte des Droits Fondamentaux de l'Union Européenne.**

Est d'abord mise en cause la protection de la vie privée reconnue à **l'article 7 de la Charte** (points 25 et 34), qui est affectée „*de manière directe et spécifique*“ (point 29): il est à ce sujet souligné que les „*données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées*“ (point 27), la Cour insistant sur le fait qu'il importe peu que „*les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence*“ (point 33) et que „*l'accès des autorités nationales compétentes aux données constituent une ingérence supplémentaire dans ce droit fondamental*“ (point 35).

Quant à la mise en oeuvre d'une dérogation aux exigences posées par **l'article 8 de la Charte** en matière de protection des données à caractère personnel (points 29 & 36), dont le régime est organisé par les directives 95/46 et 2002/58 relatives au traitement des données à caractère personnel dans le secteur des communications électroniques (point 32), la Cour estime, „*la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci*“ (point 53).

La Cour conclut que: „*l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère [...] d'une vaste ampleur*“; „*elle doit être considérée comme particulièrement grave*“; „*la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées [...] le sentiment que leur vie privée fait l'objet d'une surveillance constante*“ (point 37).

Toutefois, et ce point a été négligé – de manière délibérée ou non – par maint commentateur de l'arrêt, la Cour analyse ensuite le respect de **l'article 52 § 2 de la Charte** en vertu duquel „*toute limitation de l'exercice des droits et des libertés consacrés du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui*“. Elle analyse de ce point de vue:

- la reconnaissance de la poursuite d'un objectif d'intérêt général; et
- le respect des principes de nécessité et de proportionnalité.

Elle répond de façon positive à **la question de savoir si la directive 2006/24/CE respecte le „contenu essentiel“ des droits considérés.**

Il en est ainsi selon elle parce que „*la directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel*“ (point 39) et que les „*fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, doivent respecter certains principes selon lesquels les Etats membres veillent à l'adoption de mesures tech-*

niques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données" (point 40).

La Cour poursuit son travail d'examen, mettant ainsi en évidence que le respect du contenu essentiel des droits n'est pas suffisant en soi, mais que toutes les exigences posées par l'article 52 § 2 de la Charte doivent être respectées.

Elle s'attache en conséquence à vérifier si les atteintes aux droits fondamentaux constatées sont justifiées par la poursuite d'un objectif d'intérêt général.

Elle estime – et ce point est essentiel – que „*la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquêtes*“.

Néanmoins, elle ajoute immédiatement que „*un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte*“ (point 51). Autrement dit, **la lutte contre la criminalité organisée et contre le terrorisme, au nom de la préoccupation de sécurité intérieure, ne saurait autoriser des atteintes inutiles et inadéquates, inappropriées et injustifiées aux droits fondamentaux des citoyens européens**. En effet, comme le rappelle la Cour, „*dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci*“ (point 47).

La Cour contrôle ensuite le respect des principes de nécessité et de proportionnalité, en s'assurant d'abord que les mesures adoptées sont bien nécessaires à la réalisation de l'objectif poursuivi, et ensuite que les dispositions en cause emportent des limitations des droits fondamentaux proportionnées d'une part à l'objectif poursuivi et d'autre part aux résultats escomptés.

Elle se livre ici encore à un **contrôle strict** étant donné que: „*compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict*“ (point 48).

Pour ce qui est de **la nécessité des mesures adoptées pour atteindre l'objectif fixé**, la Cour admet que la conservation des données constitue „*un instrument utile*“ en matière de poursuites pénales (point 49)³.

Elle examine **la proportionnalité des dispositions de la directive à l'objectif matériel poursuivi**. Est rappelée l'exigence pour le législateur européen de „*prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*“ (point 54), cette exigence de prévoir de telles garanties étant „*d'autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données*“ (point 55).

Or, cet impératif n'est, aux yeux du juge de l'Union, pas respecté de façon satisfaisante par la directive 2006/24/CE, et ce pour plusieurs raisons.

Premièrement, le texte impose „*la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet*“ et „*couvre tous les abonnés et utilisateurs inscrits*“ (point 56), tant et si bien qu'elle „*concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques*“ (point 58), et par là même emporte „*une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne*“ (point 56).

³ La Cour ne s'oppose donc nullement par principe à toute rétention de données, ce qui serait irresponsable, elle estime tout simplement qu'il faut l'encadrer de conditions strictes.

Deuxièmement, **le texte n'établit aucune limitation de l'accès aux données conservées** des autorités nationales de sécurité (point 60), n'énonce aucune condition matérielle et procédurale pour l'exercice d'un tel accès (point 61), n'envisage aucun contrôle préalable par une juridiction ou une entité administrative indépendante (point 62).

Troisièmement, **le texte n'encadre pas la conservation des données** durant la période de 6 mois à 2 ans établie, puisqu'il n'opère pas de distinction entre les données conservées en catégories conçues en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées (point 63), n'impose pas de dispositifs „*permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données*“ (point 66), n'exige **aucunement** la conservation des données sur le territoire de l'Union (point 68)⁴.

Ensuite la Cour critique encore les faits que:

- le défaut de limitation de la conservation porte soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes déterminé susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, et
- le fait que la directive n'impose pas que les données en cours soient conservées sur le territoire de l'Union de sorte que le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3 de la Charte.

Aussi est-ce pour l'ensemble de ces raisons que la Cour a estimé que la directive est contraire à la Charte, alors qu'elle est trop imprécise et laisse ouverte beaucoup de questions.

*

III) L'OBJET DU PROJET DE LOI SOUS EXAMEN

Il importe de souligner que l'objet essentiel du projet de loi est de préciser les conditions dans lesquelles un juge d'instruction peut ordonner le repérage de communications.

A lire tant l'arrêt de la Cour de Justice que des articles de doctrine parus dans la suite on ne peut se défaire de l'impression qu'il y a une confusion entre la rétention de données et le repérage de données précises.

La **rétention** visée est la conservation des données recueillies par les fournisseurs de services dans le cadre de leurs activités de mise à disposition de communications électroniques au public ou de réseaux publics de communication. Il s'agit d'atteintes purement virtuelles à la vie privée des utilisateurs de tels moyens de communication.

⁴ Sur ce point il semble y avoir un malentendu majeur:

Le propre de toute enquête policière ou judiciaire est de rechercher les auteurs, coauteurs ou complices d'une infraction. Il est dès lors impossible de délimiter la rétention des données „*selon les personnes concernées*“, puisqu'on ne les connaît pas: d'où d'ailleurs le problème que les données, une fois qu'on admet le principe de la rétention de données et de repérage consécutif il est impossible de les limiter à des personnes déterminées, à moins que l'on ait l'idée – pour le moins saugrenue – d'établir des listes contenant d'une part des personnes au-dessous de tout soupçon et d'autre part des personnes suspectes (de par leurs antécédents? leur personnalité? le milieu dans lequel ils vivent?). Il s'entend qu'un tel système serait contraire aux principes les plus élémentaires en matière de protection des droits de l'homme.

La Cour constitutionnelle de Belgique a d'ailleurs fort bien vu ce problème dans son arrêt du 11 juin 2015, dans une affaire où les requérants (des avocats) faisaient grief à la législation belge en la matière de ne pas exclure du système des personnes dont l'activité tombe sous le secret professionnel, de sorte que celui-ci serait ainsi violé, la Cour ayant souligné „*que les méthodes proposées par les requérants pour séparer les métadonnées des avocats de celles du commun des mortels sont impraticables (voir notamment A.3.3.). La seule issue possible serait de renoncer à la rétention de données. C'est le tout ou rien. Voir le point A.4.5, résumant la thèse des requérants: „Quant à l'impossibilité invoquée de mettre en oeuvre une distinction selon que les données émanent de titulaires du secret professionnel ou d'autres personnes, ces difficultés ne justifieraient pas qu'une annulation pure et simple de la disposition critiquée ne puisse être prononcée afin de mettre fin à une situation discriminatoire*“.

Le même problème se pose en ce qui concerne la détermination des mesures visées à une zone géographique déterminée. S'il y a certes des situations où une telle détermination se justifie (et elle est d'ailleurs réalisée à l'heure actuelle), on ne saurait limiter la rétention de données par principe à des zones géographiques déterminées, la mondialisation du terrorisme – et les résultats de certaines enquêtes étant là pour nous le démontrer tous les jours.

D'ailleurs, tout près de nous le tueur des victimes du Musée juif de Bruxelles ne venait-il pas de Marseille où se trouvent d'ailleurs les membres de son organisation?

Une **mesure de repérage** a pour but de retrouver et d'identifier la source d'une communication, la destination de celle-ci, la date, l'heure, la durée et le type de la communication, le matériel utilisé à cette fin, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

„Seulement ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.“ (point 27 de l'arrêt de la Cour).

Cette intrusion dans la vie privée est infiniment plus grande que la simple rétention de données, même si par une mesure de repérage le contenu des informations échangées reste, par définition, parfaitement inconnu.

Il n'y donc pas lieu de confondre non plus repérage et par exemple écoutes téléphoniques.

L'article 67-1 de notre code d'instruction criminelle prescrit de manière détaillée les conditions et modalités auxquelles le juge d'instruction doit soumettre ses ordonnances relatives à une **mesure de repérage**.

*

IV) NOTRE LEGISLATION EST-ELLE CONFORME AUX CRITERES DEGAGES PAR LA COUR DE JUSTICE?

Il est un fait que notre législation en la matière est bien plus protectrice du droit à la vie privée que ne l'était la directive 2006/24/CE.

En effet notre législation prévoit un certain nombre de garanties:

- Seule une autorité judiciaire indépendante, à savoir le juge d'instruction peut par une ordonnance motivée décider un repérage.
- Le repérage est réservé, aux termes de la loi sous avis, aux autorités judiciaires donc à une autorité indépendante et impartiale qui prend sa décision sur la base d'une enquête judiciaire préalable.
- Aux termes de l'article 67-1 du code d'instruction criminelle toute personne qui a fait l'objet d'une mesure de repérage doit en être informé, au cours de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. La durée d'une mesure de repérage ne peut en principe excéder un mois sauf renouvellement.
- Tout justiciable visé dispose de la possibilité d'introduire une requête en nullité contre la mesure ordonnée et, finalement, si la mesure de repérage n'a donné aucun résultat, *„les données obtenues seront retirées du dossier de l'instruction et détruits dans la mesure où elles concernent des personnes non-inculpées“* (Alinéa final de l'article 67-1 du code d'instruction criminelle).
- Notre loi ne permet un repérage et la rétention de données dans sa suite que si le fait visé par l'instruction préparatoire emporte une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an.
- La durée de rétention de données est limitée dans notre législation à 6 mois et ne peut en aucune hypothèse s'étendre jusqu'à 24 mois (ainsi que le permettait la directive annulée).
- Le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics (Mémorial A, 2010, n° 122, page 2016) précise, conformément aux exigences de la Cour de justice les catégories de données à retenir.

S'il est exact que notre loi ne correspond pas en tous points aux critères exigés par la Cour, il n'en reste pas moins que notre législation s'en approche de très près et est de toute façon bien plus proche que des exigences „vagues“ de la directive visée. La discussion de savoir si notre législation aurait

également subi les „foudres“ d’une juridiction nationale ou internationale est certes intéressante mais dans les conditions données de nature purement académique.

*

Il importe toutefois de noter que le justiciable ne dispose d’aucune garantie si la rétention (et le repérage consécutif) est effectuée par le SREL.

A noter qu’aucune des garanties indiquées ci-avant ne figure aux paragraphes (2) et (3) de l’article 10 du projet de loi 6675 portant organisation du Service de Renseignement de l’Etat (ni la version originale du projet, ni l’avis du Conseil d’Etat n’abordent le sujet).

La question se pose dès lors s’il n’y a pas lieu de modifier ce projet sur ce point, étant donné qu’il ne saurait y avoir deux législations parallèles ayant le même objet mais accordant aux citoyens plus ou moins de droits selon le service qui ordonne la mesure!

A noter encore que les auteurs des textes semblent avoir moins de confiance dans la Justice que dans le service secret. Les dangers de ces confusions ont d’ailleurs été longuement exposés dans l’avis du soussigné du 2 avril 2015 relatif au projet de loi 6761 relatif au terrorisme.

*

V) EXAMEN DU TEXTE DU PROJET DE LOI

Ad article 1er

Pour les raisons développées ci-avant il importe de préciser les infractions pour lesquelles le juge d’instruction peut, en cas d’une instruction préparatoire, ordonner une mesure de repérage.

La Cour de justice sanctionne bien logiquement une telle „absence générale de limites“ (point 60) par l’annulation intégrale et immédiate de la directive 2006/24/CE, annulation dont les implications se révèlent très exigeantes tant pour les institutions européennes que pour les autorités nationales.

Au lieu de prévoir que les faits pour lesquels le juge d’instruction peut ordonner un repérage doivent emporter une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d’emprisonnement, le projet prévoit une liste d’infractions ce qui se justifie, du moins en principe, parfaitement.

Notre législation pénale est en effet, du point de vue des peines, trop hétéroclite et incohérente pour que le critère, permettant de procéder à un repérage, soit fixé par une référence au seuil des peines.

Les auteurs du projet se sont inspirés pour la rédaction du texte proposé, du moins dans une certaine mesure, de la liste des infractions prévues à l’annexe D de la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d’enquête européenne en matière pénale.

Si la référence à une liste d’infractions est en soit à saluer, il convient toutefois de signaler que notre législation pénale contiendra désormais plusieurs listes d’infractions permettant de recourir à l’une ou l’autre mesure procédurale, ce qui risque évidemment d’entraîner inévitablement des interférences et des confusions.

La lisibilité et la cohérence de notre législation pénale n’y gagneront rien.

La question principale est toutefois celle de savoir si les infractions énumérées au projet sont à considérer comme relevant toutes de „la criminalité grave“ visée par le point 51 de l’arrêt de la Cour de justice.

Celle-ci fait uniquement référence de manière précise au terrorisme et à la criminalité organisée.

Si la référence au terrorisme ne saurait en l’espèce donner lieu à difficultés, bien que la notion de „terrorisme“ ait obtenue, surtout ces derniers temps, des contours légaux de plus en plus flous.

La référence à la notion de „criminalité organisée“ est par contre bien plus difficile à cerner. Il s’agit en l’espèce bien plus qu’un concept relatif „modus operandi“ qu’à une infraction précise! L’existence même de ce concept est d’ailleurs régulièrement remise en cause. Il peut y avoir une criminalité organisée ayant pour objet des pommes de terre, des billes ou du chewing-gum!

A noter encore que les notions de „criminalité organisée“ recouvrent dans notre législation tant les „associations de malfaiteurs“ que les „organisations criminelles“ ont pour point commun qu’il s’agit

d'associations „en vue“ de commettre certains crimes ou délits. Il s'agit donc d'infractions par intention et non par commission.

La différence est de taille.

Reste alors l'hypothèse que la Cour de justice a eu en vue la notion de crime organisé dans son sens criminalistique, mais non juridique.

Les choses se compliquent par le fait que la Cour de justice retient tant aux points 43 que 51 que la rétention de données est un instrument utile dans la prévention des infractions et la lutte contre la criminalité et **notamment** la criminalité organisée.

En utilisant l'adverbe „notamment“ la C.J.U.E. admet le recours au repérage pour d'autres infractions d'une gravité incontestable.

Pour cette raison il convient d'examiner minutieusement la liste des infractions prévues au projet de loi, aux fins d'examiner si toutes les infractions y prévues peuvent bien être considérées comme étant d'une gravité particulière.

Cet exercice est par nature très difficile étant donné que la notion d'infraction grave n'est pas une notion juridique, et manque donc de la précision pourtant requise par principe en matière pénale. Par la force des choses la notion de „*criminalité grave*“ n'est dès lors pas objective mais subjective.

En application des articles 2, 3 et 4 de la C.E.D.H., signée à Rome le 4 novembre 1950 le droit à la vie (y compris la défense de toute personne contre la violence illégale) l'interdiction de la torture et l'interdiction de l'esclavage et du travail forcé sont indubitablement à considérer comme les droits de l'homme les plus fondamentaux, de même que toutes les atteintes à la vie et atteintes graves à l'intégrité physique.

Le système de la liste d'infractions montre d'ailleurs en l'espèce ses limites en ce qu'elle risque toujours d'être incomplète. Il est ainsi, à titre d'exemple, indiscutable que des infractions en rapport avec des réseaux de pédophilie relèvent de la criminalité grave, mais ne figurant pas sur la liste.

Qu'il y ait possibilité de repérage et de rétention de données dans ces cas de figure ne saurait donner lieu à discussion.

Pour les raisons exposées ci-avant les infractions énumérées au point 2) de l'article premier de la loi sous examen et portant modification de l'article 67-1 sous 3), 4), 18), 19), 20), 21), 30) et 33) doivent figurer sans aucun doute sur la liste des infractions susceptibles de faire l'objet d'une mesure de repérage.

Il devrait en être de même pour les infractions énumérées sous 1), 7), 13), 23) et 29).

Par contre pour les infractions énumérées aux points 8), 9), 10), 11), 15), 17), 25), 26), 27), 28) et 31) il s'agit d'infractions ayant exclusivement pour objet l'appropriation d'objets matériels. En l'espèce à titre d'illustration, de ce que les listes d'infraction sont toujours incomplètes, la question se pose encore pourquoi, à titre d'exemple, le délit d'initiés n'y figure pas.

S'agit-il en l'espèce et par principe d'infraction d'une gravité objective réelle?

Voilà bien le problème.

Si l'on se place du côté des droits de l'homme et de la philosophie sous-jacente de l'arrêt de la Cour de justice on devrait conclure à ce que ces infractions ne sauraient faire l'objet d'une mesure de repérage.

Par contre si l'on estime qu'il y a lieu de sanctionner l'appropriation illicite de biens et de s'assurer à cette fin de tous les moyens de preuves techniquement disponibles l'on n'hésitera pas à trouver évident que les auteurs de ces infractions puissent faire l'objet d'une mesure de repérage.

Dans ce contexte, il importe de relever que la Cour européenne des droits de l'homme a précisé en 2010 dans une affaire Uzun contre Allemagne (arrêt du 2 septembre 2010, n° 35623/05) que „*eu égard au risque d'abus inhérent à tout système de surveillance secrète, de telles mesures doivent se fonder sur une loi particulièrement précise, en particulier compte tenu de ce que la technologie disponible devient de plus en plus sophistiquée*“ (point 61 de l'arrêt).

Les infractions énumérées sous 22), à savoir le harcèlement et les atteintes à la vie privée sont certes du point de vue de la victime d'une gravité subjective réelle. Mais peut-on les considérer comme étant d'une gravité objective réelle? Au moins un doute est permis.

Les infractions énumérées au point 14) et relatives à la cybercriminalité donnent lieu à une observation particulière.

En effet en application de l'article 3 de la loi du 18 juillet 2014 relative à la cybercriminalité (Mémorial A, 2014, n° 133, page 2134) au moins cinq infractions nouvelles ont été introduites dans notre code pénal qui ne sont cependant en rien énumérées dans le projet de loi sous examen.

Il s'y ajoute qu'au point 7) du même article 3 de la loi du 18 juillet 2014 on rend punissable ceux qui ont sciemment facilité, par tout moyen, la justification mensongère de la nature, de l'origine de l'emplacement, de la disposition, du mouvement ou de la propriété des biens visés à l'article 32-1 du code pénal, alinéa 1 premier sous 1), forment l'objet ou le produit, direct ou indirect, des infractions y visées.

Suit une longue, très longue liste d'infractions qui peuvent, en application de la disposition visée ci-avant, faire l'objet d'une mesure de repérage, à condition que l'origine des biens ait été trafiquée par un des moyens énumérés ci-avant.

Ceci n'est pas sans rappeler le fameux cheval de Troie.

Ce qui semble a priori important et impressionnant ce n'est pas le contenu mais le contenant!

Or, l'inverse est vrai.

Le fait à la base de bien matériel ou immatériel ce qui a ensuite été trafiqué quant à son origine est infiniment plus grave que le fait que par une manipulation informatique l'origine réelle du bien a illicitement été trafiqué.

Il ne semble d'ailleurs guère logique de ne pas permettre un repérage pour de nombreuses infractions, mais de le permettre si elles ont ensuite fait l'objet d'un acte de cybercriminalité.

Il résulte de l'examen de l'article visé qu'en fin de compte il ne saurait guère y avoir d'infractions ayant fait l'objet depuis l'entrée en vigueur de la loi du 30 mai 2005 d'une mesure de repérage qui ne figure pas dans l'énumération. La loi serait-elle, sur ce point, un coup d'épée dans l'eau?

Le soussigné fait encore siennes les observations purement juridiques contenues dans l'avis de la Cour Supérieure de Justice.

Ad article 2 point 4)

Aux termes de cette disposition „*les données visées*“ sont conservées sur le territoire de l'Union européenne.

Il est certes exact que la Cour de justice considère dans son arrêt que les données conservées ne sauraient quitter le territoire de l'Union européenne, mais ceci en raison du fait que la directive visée ne contient aucun contrôle avant la transmission de ces données à un territoire situé en dehors de l'Union européenne.

Or, à titre d'exemple, le Grand-Duché de Luxembourg s'apprête à ratifier le „*Memorandum of understanding between the Government of the Grand-Duchy of Luxembourg and the United States of America for the exchange of terrorism screening information*“ signé à Luxembourg le 20 juin 2012, qui prévoit la possibilité d'échanger les données telles que celles visées au projet.

Le projet de ratification prévoyant des mécanismes de contrôle, le texte proposé règle la situation pour notre pays.

Il y a donc lieu de reformuler la disposition visée.

Il s'entend d'ailleurs que dans un domaine comme le terrorisme l'échange de données au-delà des pays de l'Union européenne, est indispensable.

Aurait-on oublié, à titre d'exemple, que les auteurs des attentats du 11 septembre 2001 aux Etats-Unis vivaient avant les attentats, de manière cachée, en Allemagne?

Interdire de manière absolue le résultat d'un repérage n'est ni cohérent, ni raisonnable au regard du grave problème actuel du terrorisme.

Ad articles points 1) et 2)

Les dispositions ne donnent pas lieu à observation étant donné qu'elles tendent, à bon droit, à apporter des précisions à notre droit allant dans le sens préconisé par la Cour de justice dans l'arrêt visé.

Il se pose toutefois un autre problème assez délicat.

En effet à l'heure actuelle se trouve également dans la procédure législative le projet de loi n° 6675 portant notamment organisation du Service de Renseignement de l'Etat.

Or, aux termes de ce projet (tant du projet initial que du texte amendé présenté par le Gouvernement suite à l'avis du Conseil d'Etat):

„Le SRE est autorisé à procéder au repérage de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications“;

„en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou le fournisseur d'un service de télécommunications. La durée de cette mesure de recherche ne pourra se reporter qu'à une période maximale de six mois (...), sans préjudice de renouvellement (article 10, paragraphe (2), devenu article 7, paragraphe (2))“.

Selon l'article 67-1, paragraphe (1) alinéa 5 le juge d'instruction peut ordonner une mesure de repérage pour une durée d'un mois, également renouvelable.

La question qui mérite examen est celle de savoir si de par les renouvellements successifs les données ne sont pas retenues sur une période très longue, ce qui a, le cas échéant, pour conséquence que toutes les données collectées seront retenues très longtemps.

Il ne faut pas non plus perdre de vue que dans le genre de criminalité visé, on procède par algorithmes, c'est-à-dire, si on part de l'utilisateur „A“, qu'on croit mêlé au terrorisme, on veut également savoir avec qui son correspondant „B“, est en relation, lequel est un contact régulier de „C“, etc., etc., pour voir finalement s'il y a également des relations entre, par exemple, „F“, „E“ et „A“, de sorte que toutes ces personnes sont soupçonnées d'être mêlées au terrorisme.

Pour cette raison il y a lieu de retenir toutes ces données puisqu'on recherche bien tous les contacts inconnus de „A“.

Pour cette raison on risque de retenir au-delà d'un délai de 6 mois une quantité énorme de données.

*

VI) OBSERVATIONS FINALES

En l'espèce il s'agit d'une importante question de politique criminelle, le concept étant pris en l'espèce au sens plein du mot, à savoir, pour reprendre la définition de Madame la Professeure Mireille Delmas-Marty:

„... elle (la politique criminelle) comprend l'ensemble des procédés par lesquels le corps social organise les réponses à la criminalité.

Son but essentiel est le maintien de l'ordre social. Elle consiste en des mesures préventives (éducation, famille, emploi, etc.) et des mesures répressives (emprisonnement, etc.). C'est un art difficile qui recherche l'équilibre entre l'efficacité de ces mesures et les effets pervers causés par elles, en particulier les atteintes aux droits et libertés fondamentaux des citoyens.“.

Il s'agit de faire un choix politique, notion prise au sens noble du terme. Ce choix s'opère entre les impératifs non conciliables de la liberté (entendue dans le présent contexte comme respect du droit à la vie privée) et de la sécurité.

Soit on cherche à élucider le plus grand nombre possible d'infractions⁵, soit l'on se limite, par respect, pour la protection de la vie privée, aux seules infractions portant atteinte aux valeurs essentielles pour permettre une vie commune.

La question est d'autant plus importante que le procédé visé est à la fois fort efficace pour trouver les auteurs d'infractions qu'invasive pour la vie privée des citoyens.

Une certaine modération semble se recommander pour les raisons exposées par la Cour de justice dans son arrêt „Digital Rights“.

Il s'entend que plus la liste des infractions se limite à des infractions réellement graves moins il y a lieu d'attacher une importance majeure aux problèmes de la durée de conservation des données.

Le Procureur général d'Etat,

Robert BIEVER

⁵ Sauf évidemment les infractions mineures, telles les contraventions.

