

Criminalité financière et cybercriminalité

La **criminalité financière** recouvre différentes infractions : la corruption, le blanchiment d'argent, la fraude sociale et la fraude fiscale. Ces infractions partagent une logique sociale commune : bien qu'elles soient d'une ampleur importante dans nos sociétés et qu'elles menacent directement l'équilibre économique et les valeurs démocratiques, elles sont quelque peu « *invisibilisées* » pour le citoyen qui paraît indifférent face à des millions d'euros détournés, face à cette « *criminalité sans victime* », cette « *victime virtuelle qu'est l'Etat* ».

Une analyse sociologique récente sur les élites délinquantes révèle l'ambiguïté de la réaction sociale : « *plus le dommage est tangible et important (à plus forte raison s'il y a atteinte à une personne) plus la gravité sera élevée. À l'inverse, les transgressions aux faibles impacts (surtout économiques) ou aux conséquences abstraites (fraude fiscale) se voient toujours attribuer une faible gravité* »⁷². Le caractère passif ou le manque d'empathie du citoyen peut s'expliquer par « *l'absence de personnalisation des victimes qui empêche toute empathie* »⁷³, à l'inverse de l'affaire Dutroux, mais aussi par la complexité technique de ce type de criminalité.

La **corruption** est le fait d'accepter ou proposer des avantages personnels facilité par une fonction publique ou privée.

Le **blanchiment d'argent** est lui l'infraction majeure de la criminalité financière, allant du fraudeur fiscal aux groupes organisés de trafic de drogues, et vise à profiter en toute impunité de fonds issus de la criminalité.

La **fraude sociale** vise prioritairement le dumping social et le travail non déclaré et l'assujettissement frauduleux à la sécurité sociale (fausses déclarations ONSS, fausses fiches de paie, accès à des prêts bancaires, regroupement familial etc.). Elle est, de ce fait, parfois liée à la traite et au trafic des êtres humains, mais nuit surtout aux droits des travailleurs et indépendants et induit une concurrence déloyale.

La **fraude fiscale** se traduit par le non-respect des obligations en matière d'impôt sur le revenu ou de TVA. D'autres typologies de fraude doivent elles aussi être approfondies.

La **cybercriminalité** se définit par l'utilisation abusive de l'automatisation et de données automatisées⁷⁴. La fraude à la carte de paiement en fait partie.

⁷² Lascoumes, P et Nagels, C., Sociologie des élites délinquantes, éd. Armand Colin, 2014, p. 63.

⁷³ Claise, M., Essai sur la criminalité financière, éd. Racine, 2015, p. 36.

⁷⁴ Cf. définition du PNS (p. 53) : « La cybercriminalité ou le cybercrime est un délit d'utilisation abusive, en tant que moyen, de l'automatisation et de données automatisées, pouvant viser également les systèmes informatiques ou les données y étant enregistrées. »

Stratégie

Les parties prenantes du présent plan entendent travailler de manière transversale, notamment avec les services fédéraux spécialisés, à l'élaboration d'une connaissance plus approfondie en matière de fraude et de criminalité financière, ainsi qu'à sa répression. Un travail parallèle de sensibilisation de la population à l'importance de cette forme de criminalité reste nécessaire.

En matière de fraude fiscale, les parties prenantes au présent plan entendent renforcer la coopération entre les administrations fiscales et les parquets, entre les autorités compétentes (Fédéral - Régions) en vue d'un contrôle renforcé et d'une politique réactive cohérente (cf. NCSI M11, 4.4.2).

Les infractions suivantes seront considérées en priorité :

- **De fraude à l'impôt sur les revenus ;**
- **De fraude organisée à la TVA ;**
- **De fraude sociale :** en cette matière, davantage de contrôles seront prévus et la répression favorisera la voie administrative.

Une attention particulière aux **travailleurs victimes de fraude sociale** permettra, le cas échéant, de les indemniser dans le cadre de leur régularisation, en complément de l'approche développée dans la partie « traite des êtres humains ».



Suivi

M8.10 : Prévoir, au niveau national, un **suivi** étroit des nouvelles tendances par l'OCS (Cellule de soutien fraude carrousel TVA) et en informer les services d'inspection de l'ISI, les parquets et la police fédérale, par le biais de séances de formation (cf. NCSI M1, 4.4.2).

Prévention

M8.1 : Prévoir des **formations** spécifiques :

- Formation sur la **criminalité financière**, en prenant en compte la problématique du transfert de compétences et de connaissance des dossiers au sein des services (car les dossiers financiers sont souvent très longs dans le temps). Ces formations veilleront également à une association des autres acteurs partenaires dans ces matières ;
- Formation multidisciplinaire pour améliorer les connaissances et compétences des services communaux et de police, via un échange de bonnes pratiques relatives à l'approche des **sociétés à but commercial créées sous le statut d'ASBL**. Effectuer une étude de faisabilité en vue de proscrire l'exercice de certaines activités commerciales sous le couvert du statut d'ASBL ;

M8.2 : Stimuler une plus grande **collaboration**, favoriser et renforcer les **échanges d'informations** entre les services d'inspection sociale, les services de police et les services publics compétents en matière de fraude ;



Criminalité financière et cybercriminalité Fraude

Réaction

M8.3 : Lutter contre le **dumping social** dans le cadre de l'adjudication des **marchés publics** (secteur du nettoyage, chantiers de la construction...) en sensibilisant et formant les administrations compétentes en la matière ;

M8.4 : En matière de fraude fiscale et sociale, assurer une application cohérente et concertée du **modèle una via** (choix entre la voie administrative et la voie judiciaire), selon le respect des principes de subsidiarité et de non bis in idem, en vue d'une **affectation optimale des moyens** dont l'administration fiscale, la police et le ministère public disposent (cf. NCSI M7, 4.4.2). En matière de fraude sociale, porter une attention particulière pour les faux en droit pénal social⁷⁵ (cf. NCSI M5, 4.4.1) ;

M8.5 : Vis-à-vis de la fraude sociale, appliquer des **méthodes de recherche affinées**⁷⁶, renforcer les **collaborations** entre entités fédérées et internationales et mettre en œuvre de manière dissuasive toutes les **sanctions** prévues par la législation en cas d'occupation illégale de travailleurs étrangers ou d'exercice illégal d'une activité indépendante par un étranger (cf. NCSI M4, 4.4.1) ;

M8.6 : Adjoindre les **services de contrôle régionaux** à l'adoption d'une approche administrative plus sévère de la fraude sociale prévue par la Note Cadre (cf. NCSI M7, 4.4.1) ;

M8.7 : Exécuter de manière optimale les **amendes administratives** imposées aux contrevenants étrangers (via le **système d'information du marché intérieur** (IMI) – chapitre 6 de la direction d'exécution) (cf. NCSI M6, 4.4.1) ;

M8.8 : Dans les secteurs concernés, effectuer des **contrôles**⁷⁷ dans le cadre des cellules d'arrondissement, tel que défini dans le plan d'action du SIRS (construction, transport, HORECA...) (cf. NCSI M3, 4.4.1) ;

M8.9 : Faciliter et renforcer les **collaborations** entre les services d'inspection et la police locale, notamment lors des **contrôles** sur le terrain ;

⁷⁵ Cf. articles 230-236 du Code pénal social.

⁷⁶ Cf. COL 07/2014 du 29 avril 2014 relative à la lutte contre le dumping social et COL 12/2012 du 22 octobre 2012 relative à la politique criminelle en matière de droit pénal social.

⁷⁷ Ces contrôles appuient les politiques régionales en matière d'emploi.

Suivi

M8.15 : Etablir une **image** des cybermenaces et des cyberincidents qui se produisent en Région bruxelloise.

Prévention

M8.11 : **Développer la prévention** et sensibiliser aux **risques** encourus à l'usage des technologies de l'information et de la communication (TIC) :

- Mettre à disposition les informations sur les **leçons tirées** des cyberincidents (bonnes pratiques) ;
- Définir pour les **entreprises des règles de « bonnes conduites »** génériques en matière de sécurité ; définir une politique régionale en ce sens et délivrer un **label régional** (certification Sécurité IT) aux entreprises s'engageant dans ce processus ;
- Développer une campagne de sensibilisation du **public** à la cybersécurité ;

M8.12 : **Sensibiliser les acteurs régionaux** de la prévention et de la sécurité :

- A la promotion d'une **utilisation responsable d'internet par les jeunes** (via par exemple, le projet fédéral iCoach⁷⁸) ;
- Au **renforcement des équipements régionaux** en matière informatique (protection des données, disponibilité de l'infrastructure et développer des applications telles que la vidéo-protection et des outils de partage d'informations) ;
- A l'utilisation de **méthodes de renseignement** qui ont recours à des sources ouvertes, disponibles publiquement (*Open Source Intelligence*) ;
- A l'importance de **désigner un point de contact IT** dans chaque administration régionale, zonale et communale pour relayer les informations qui seront diffusées par le Centre de Cybercriminalité belge (CCB) ;

M8.13 : En matière de **formation** :

- Développer un centre de connaissances et des partenariats avec des universités pour certaines formations spécialisées ;
- Elargir l'offre de formations relatives à la cyber-sécurité au sein de l'Ecole des métiers de la sécurité ;

Criminalité
financière et
cybercriminalité
Cybercriminalité

Réaction

M8.14 : Renforcer les capacités de recherche sur le darknet afin notamment de lutter de manière proactive contre le développement de divers phénomènes criminels (trafic de stupéfiants, trafic d'armes, prévention et lutte contre le terrorisme et le radicalisme) et favoriser l'échange des informations qui en résultent entre les services compétents ;