CONTRÔLE RESTREINT

RAPPORT DE CONTRÔLE AUPRÈS UNE ZONE DE POLICE DE L'ARRONDISSEMENT DE LIÈGE PAR L'ORGANE DE CONTRÔLE DE L'INFORMATION POLICIÈRE DANS LE CADRE DE SA COMPÉTENCE DE SURVEILLANCE ET DE CONTRÔLE

Référence : DIO22004

Table de matières

1 INTRODUCTION

1. Les Ministres de la Justice et de l'Intérieur ont demandé à l'Organe de contrôle de l'information policière (ci-après dénommé « COC ») de mener un contrôle thématique[1] (par échantillonnage) sur l'application d'une partie du dispositif

[1] Le COC fait la distinction entre plusieurs formes de contrôle ou de supervision :
- **Contrôle global** : il s'agit d'une enquête de contrôle qui s'accompagne d'une ou plusieurs visite(s) approfondie(s) sur le terrain ou de visites où la portée de la surveillance est très large.

dit 'Salduz' au sein de la police intégrée. Plus précisément, le contrôle porte sur l'utilisation de caméras de surveillance et/ou d'audio pendant ou à la suite de la concertation confidentielle entre le client (suspect/personne inculpée) et son avocat.

Dans ses réponses apportées au questionnaire général faisant partie de ce contrôle thématique, la zone de police de l'Arrondissement de Liège (ZP de l'Arrondissement de Liège) indique « *Nos locaux d'audition enregistrent la vidéo et le son en permanence, mais le contenu de ces enregistrements n'est accessible qu'au service de contrôle interne. Le fonctionnaire de police qui procède à l'audition ne prend donc aucune décision* ».
De plus, la ZP de l'Arrondissement de Liège avait répondu « *oui* » à la question nr 4 du questionnaire, à savoir :
« Est-ce que la salle de la concertation confidentielle est utilisée comme salle d'audition habituelle? »

Des informations obtenues[2] auprès de la zone de police Arrondissement Liège, il s'avère que :

- il n'y a pas de directive concernant cet enregistrement. Le système de vidéosurveillance a juste été déclaré dans le registre des bases de données (RegPol) ;
- l'avocat n'était/n'est pas systématiquement prévenu de l'enregistrement.

Compte tenu de ses compétences en tant que service de contrôle externe et autorité de contrôle compétente en matière de traitement de données par la police intégrée, structurée à deux niveaux (GPI), et malgré le fait que le contrôle thématique ne visait pas *a priori* des entités de police individuelles, l'Organe de contrôle de l'information policière (Organe de contrôle ou COC), a décidé de procéder à une visite sur place de la zone de police de l'Arrondissement de Liège dans le cadre d'un contrôle restreint.

1.1 Les compétences de l'Organe de contrôle de l'information policière

2. Dans le cadre de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD)[3], le COC a été réformé et est devenu une autorité de contrôle à part entière, outre ses compétences de contrôle existantes en matière de traitement opérationnel de l'information tel que prévu dans la loi du 5 août 1992 sur la fonction de police (LFP). L'article 71 §1 et le titre 7 LPD définissent les missions et compétences du COC. Ils renvoient également aux missions de contrôle spécifiées dans les articles 44/1 à 44/11/14 LFP relatifs au traitement de l'information par les services de police. En ce sens, l'Organe de contrôle est investi d'une mission de surveillance et de contrôle. Cela signifie qu'au-delà de la protection de la vie privée et des données à caractère personnel, le COC prête également attention à des éléments tels que l'efficience et l'efficacité du traitement de l'information et de l'intervention policière. En vertu de la réglementation susmentionnée, le COC a par conséquent une compétence générale de surveillance sur tous les traitements de données (à caractère personnel), tant opérationnels que non opérationnels, par la GPI.

- **Contrôle thématique** : comme son nom l'indique, une enquête est menée sur un thème spécifique, ce qui permet à la fois une recherche documentaire et/ou des visites sur place.

- **Contrôle technique** : ces contrôles se limitent principalement à vérifier la légalité, l'exhaustivité et l'exactitude des saisies et des traitements dans les banques de données policières.

- **Contrôle restreint** : ces contrôles portent sur un ou seulement quelques (sous-)aspect(s) du traitement des données policières opérationnelles ou non-opérationnelles.

- **Contrôle international** : il s'agit des éventuelles enquêtes internationales auxquelles le COC collabore ou qui s'inscrivent dans le cadre de ses obligations internationales.

- **Contrôle particulier** : il s'agit d'enquêtes et de contrôles dans des domaines particuliers, tels que les contrôles annuels des banques de données communes sur le terrorisme et l'extrémisme.

2 Échange de mail entre le COC et la ZP Arrondissement Liège du 24-01-2022, 09-02-2022 et 15-02-2022.

[3] M.B. 5 septembre 2018. Elle contient également des dispositions d'application du Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données), ci-après la LPD, et la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou aux fins de l'exécution de sanctions pénales, et de libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

Le COC est compétent notamment pour les services de police[4], pour l'Inspection générale de la police fédérale et locale (AIG)[5] et pour l'unité d'Information des Passagers (UIP)[6]. La compétence du COC en ce qui concerne les services de police couvre à la fois les activités de traitement opérationnelles (Titre 2 LPD) et non opérationnelles (RGPD)[7].
En ce qui concerne la mission de contrôle, le COC est chargé de contrôler le traitement des informations et des données visées à l'article 44/1 LFP, en ce compris celles introduites dans les banques de données visées à l'article 44/2 de la même loi. Le COC est également chargé de toutes les autres missions qui lui sont confiées par ou en vertu d'autres lois.

Dans ce cadre, le COC procède à des constatations et peut avoir recours à des demandes, des recommandations, des mises en garde et/ou des mesures correctrices (des injonctions contraignantes) comme «*ultimum remedium* » et/ou si le COC constate des infractions aux lois et réglementations.

Le COC est également chargé de vérifier le respect des règles concernant l'accès à la Banque de données Nationale Générale (BNG) et à sa consultation directe, ainsi que le respect de l'obligation, visée à l'article 44/7, paragraphe 3 LFP, pour tous les membres des services de police, d'alimenter cette banque de données.

Le COC vérifie également le bon fonctionnement de la BNG et la procédure de traitement des données et informations qu'elle contient afin de déterminer si celle-ci est conforme aux dispositions des articles 44/1 à 44/11/13 LFP ainsi qu'à leurs mesures d'application.

En ce qui concerne l'utilisation de caméras non visibles, le COC agit comme une sorte de commission « MPA »[8]. Selon l'article 46/6 LFP, toute autorisation et modification de l'utilisation non visible de caméras dans les cas visés à l'article 46/4 doit être notifiée au COC, sauf lorsque l'utilisation de caméras est effectuée sous l'autorité d'un magistrat. Dans ce cadre, le COC examine si les conditions de la décision de mise en œuvre ou de la prolongation de la mesure sont remplies.

En outre, le COC traite les plaintes relatives à l'application de la législation qui concerne le traitement des données à caractère personnel par les service de police [9]. A cette fin, les membres du COC et les membres du service d'enquête (DOSE)[10] disposent de pouvoirs d'enquête et des mesures correctrices peuvent être prises[11].

Certaines décisions du COC peuvent faire l'objet d'un recours dans un délai de 30 jours devant la Cour d'Appel du lieu de résidence ou du siège social du plaignant, qui traitera l'affaire comme une procédure interlocutoire conformément aux articles 1038, 1040 et 1041 du Code judiciaire[12].

2 ORGANISATION ET MÉTHODOLOGIE DU CONTRÔLE RESTREINT

2.1 Contexte général

3. Le 18-05-2021, les Ministres de la Justice et de l'Intérieur ont demandé au COC de mener un contrôle thématique sur l'application d'une partie du dispositif Salduz au sein de la police intégrée. Plus précisément, le contrôle porte sur l'utilisation de caméras de surveillance et/ou d'audio pendant ou à la suite de la concertation confidentielle entre le client (suspect/personne inculpée) et son avocat.

La méthodologie de l'enquête consistait en l'envoi d'un questionnaire général à la GPI (1) et en la réalisation de visites sur place (2).

[4] Tel que défini à l'article 2, 2° de la loi du 7 décembre 1998 organisant un service de police intégré structuré à deux niveaux (article 26, 7°, a) LPD).
[5] Tel que défini à l'article 2 de la loi du 15 mai 2007 relative à l'Inspection générale contenant diverses dispositions concernant le statut juridique de certains membres des forces de police (article 26, 7°, d) LPD).
[6] Conformément au chapitre 7 de la loi du 25 décembre 2016 sur le traitement des données des passagers (art. 26, 7°, f) LPD).
[7] Art. 4 § 2, quatrième alinéa, de la loi du 3 décembre 2017 instituant l'Autorité de protection des données.
[8] **M**éthodes **P**articulières en police **A**dministrative.
[9] Art. 240, 4° et 247 LPD.
[10] **D**ienst **O**nderzoeken / **S**ervice d'**E**nquête.
[11] Art. 244 et 247 LPD.
[12] Art. 248 LPD.

Le 21-06-2021, le questionnaire a été envoyé vers les 235 entités de la GPI. Le 12-08-2021, un rappel a été envoyé au 50 entités qui n'avaient pas encore répondu. La zone de police de l'Arrondissement de Liège a répondu le 19-08-2021, en mentionnant « *Nos locaux d'audition enregistrent la vidéo et le son en permanence, mais le contenu de ces enregistrements n'est accessible qu'au service de contrôle interne. Le fonctionnaire de police qui procède à l'audition ne prend donc aucune décision* ».

2.2 Contexte particulier et méthodologie

4. Le 24-01-2022, après avoir effectué les devoirs d'analyse et plusieurs visites sur place dans le cadre global du contrôle tel que sollicité par les Ministres de l'Intérieur et de la Justice, le COC a procédé au traitement de la réponse de la zone de police de l'Arrondissement Liège afin d'obtenir de plus amples informations.

Une question a alors été posée le 24-01-2021 à la zone de police de l'Arrondissement de Liège. En tenant compte de la situation particulière et des conséquences des inondations de juillet 2021 auxquelles la zone de police de l'Arrondissement de Liège a été confrontée, le COC a accepté un certain délai de réaction. Le 09-02-2022, n'ayant pas eu de réponse, le COC s'est enquis auprès de la zone de police de l'Arrondissement de Liège de l'état de la situation. Le 15-02-2022, la zone de police de l'Arrondissement de Liège a répondu que :

- « *il n'y a pas de directive concernant cet enregistrement. Le système de vidéosurveillance a juste été déclaré dans le registre des bases de données (RegPol) ;*
- *l'avocat n'était pas systématiquement prévenu de l'enregistrement.* »

Le 16-02-2022, le COC a accusé bonne réception des réponses de la zone de police de l'Arrondissement de Liège.

Le 28-02-2022, le COC a décidé de procéder à une visite sur place de la zone de police de l'Arrondissement de Liège dans le cadre d'un contrôle restreint.

Le 02-03-2022, le COC a envoyé par mail une lettre annonçant une courte visite des lieux le 09-03-2022 à 10.30 h dans le cadre de l'utilisation policière des caméras dans le bâtiment de police. La présence d'une personne autorisée ainsi que d'un expert en la matière a été sollicitée.

Le 02-03-2022, la zone de police a accusé bonne réception du mail et de la lettre dans laquelle la visite était annoncée.

Le 09-03-2022 entre 10.30 et 12.00 h, le COC a effectué la visite. La visite s'est déroulée en trois parties :

1. une introduction du cadre général ;
2. une courte visite des lieux dans le cadre des objectifs ;
3. un interview relative à l'utilisation des caméras à des fins policières dans le bâtiment de police ;
4. La sélection d'un échantillon en présence du COC d'images traitées venant des caméras utilisées dans le bâtiment de police.

3 CADRE JURIDIQUE

3.1 Surveillance par caméras

3.1.1 Fondement juridique

5. Depuis la loi d'adaptation de la LFP du 21 mars 2018, la décision de placer des caméras dans les espaces publics ne peut plus être prise que par une autorité publique, comme la commune[13]. Lorsque la police utilise une surveillance par caméras, les dispositions de la LFP sont applicables sauf lorsque l'utilisation de caméras est régie par une autre législation[14].

3.1.2 Responsable du traitement

6. Dans le droit relatif à la protection des données, un rôle important est dévolu au « *responsable du traitement* ». Il s'agit de « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »[15]. En ce qui concerne les activités de traitement dans le cadre des missions de police administrative et judiciaire, le responsable du traitement est défini dans la LPD comme « *l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance* »[16]. Par « *autorité compétente* », il faut entendre « *a) les services de police au sens de l'article 2, 2°, de la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux* »[17].

7. Bien que le responsable du traitement dans la LFP se voie attribuer un rôle (spécifique) à certains égards, ce n'est pas le cas en ce qui concerne l'utilisation de caméras. Comme indiqué précédemment, le responsable du traitement est un acteur essentiel dans le traitement des données à caractère personnel. Il doit en effet démontrer que les données à caractère personnel sont traitées conformément au cadre légal. Lui, son préposé ou mandataire, est aussi la personne à laquelle des mesures correctrices éventuelles peuvent être imposées ou qui peut être poursuivi pénalement[18]. Le chef de corps est le responsable du traitement pour l'enregistrement d'images de caméras dans une banque de données technique locale[19].

Le chef de corps est aussi le responsable du traitement pour les banques de données particulières[20]. Dans les banques de données particulières, sont enregistrées des données qui ne sont pas susceptibles d'être reprises dans la BNG bien qu'elles aient une nécessité opérationnelle. Des exemples d'une banque de données particulière sont (1) l'enregistrement de numéros de téléphone ou de données ANPR qui sont recueillis dans le cadre d'une instruction pénale[21] et (2) des images de caméra classiques. Il s'agit de données en rapport avec des missions de police administrative et judiciaire mais elles ne doivent pas *ipso facto* être enregistrées/résumées dans la BNG[22]. En ce qui concerne ces dernières, nous renvoyons à l'article 25/6 de la LFP qui stipule seulement que les informations et les données à caractère personnel doivent pouvoir être conservées 12 mois maximum[23]. Un responsable du traitement n'est cependant pas désigné pour la conservation des données.

L'Organe de contrôle estime qu'il s'agit (également) d'une banque de données particulière de telle sorte que le chef de corps doit être considéré comme le responsable du traitement. L'article 44/4 § 1er, 3e alinéa de la LFP stipule en effet que les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont fixé les objectifs et les moyens relatifs à ces banques de données particulières sont les responsables du traitement pour les banques de

[13] Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, M.B. 16 avril 2018.
[14] Comme le contrôle de tronçon, qui relève de l'application de la loi du 16 mars 1968 relative à la police de la circulation routière (Doc. parl. Chambre 2017-2018, n° 54-2855/001, 9).
[15] Art. 4. 7) du RGPD.
[16] Art. 26, 8° de la LPD.
[17] Art. 26, 7° de la LPD.
[18] Voir les articles 221 et 222 de la LPD. Concrètement, l'Organe de contrôle peut notamment prendre les mesures suivantes (art. 25.2, RGPD) : - donner un avertissement ; - donner une réprimande ; - ordonner de mettre les opérations de traitement en conformité avec le cadre légal dans un délai déterminé ; imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement.

[19] Art. 44/11/3*sexies* § 1, 2e alinéa de la LFP.
[20] Article 44/4 § 1, troisième alinéa de la LFP.
[21] MERCURE.
[22] Art. 44/11/3 de la LFP.
[23] Remarquons, par souci d'exhaustivité, que la LFP n'impose pas de délai de conservation ferme pour les données qui sont enregistrées dans les banques de données particulières (art. 44/11/3, §4 de la LFP). Étant donné que l'article 25/6 de la LFP impose un maximum de 12 mois, le délai maximum est ainsi déterminé aussi pour cette banque de données particulière.

données particulières qu'ils constituent. La désignation du chef de corps comme responsable du traitement s'inscrit par ailleurs dans l'esprit des dispositions de la LFP relatives à la constitution de banques de données locales. Selon l'article 25/5 de la LFP, l'utilisation de caméras a lieu sur décision et sous la responsabilité du fonctionnaire de police compétent. Si ce n'est pas le chef de corps, le fonctionnaire de police compétent agit sous la responsabilité du chef de corps. En effet, le chef de corps, en vertu de l'article 44 de la loi sur la police intégrée, est responsable de l'exécution de la politique policière locale, et plus particulièrement de l'exécution du plan zonal de sécurité et assure la direction, l'organisation et la répartition des tâches au sein du corps de police locale et l'exécution de la gestion de ce corps[24].

Le chef de corps est donc le responsable du traitement en ce qui concerne toutes les formes d'utilisation de caméras dans sa zone de police.

3.1.3 Exigences procédurales

8. Avant qu'un service de police ne puisse installer des caméras de surveillance sur le territoire d'une commune, il a besoin à cet effet de l'autorisation préalable de principe du conseil communal[25]. Toutefois, une autorisation n'est pas nécessaire pour l'utilisation de caméras dans des lieux fermés dont la police elle-même est le gestionnaire, comme un commissariat de police[26]. Il importe de préciser que, lorsque l'autorisation du conseil communal a déjà été obtenue avant la modification de loi du 21 mars 2018 en application de la loi sur les caméras de 2007, il ne faut pas obtenir une nouvelle autorisation du conseil communal[27]. Cette autorisation initialement obtenue reste donc valable. La même autorisation ne peut toutefois pas être employée pour l'utilisation de nouveaux types de caméras qui ont été introduits par la loi du 21 mars 2018. C'est ainsi que la LFP impose des conditions spécifiques à l'utilisation de caméras fixes temporaires sur lesquelles le conseil communal doit se prononcer[28]. Dans ce cas, il faut donc obtenir une autorisation nouvelle, ou complémentaire, du conseil communal.

3.1.4 Délai de conservation des images

9. Les images des caméras peuvent être conservées pour une durée n'excédant pas douze mois[29]. La loi ne fixe pas de délai minimum. En ce qui concerne les images de caméra classiques, la LFP ne spécifie pas sur quel support de données les images doivent être enregistrées. Par conséquent, il est indiqué que le chef de corps précise dans le registre relatif au traitement de données à caractère personnel, tel que visé dans l'article 55 de la LPD (voir numéro 3.3.8), sur quel support de données les images sont enregistrées. Ce support de données doit être accessible pour l'Organe de contrôle.

3.1.5 Accès aux images

10. L'accès aux images dépend de la finalité et est réglé de la même manière tant pour la surveillance par caméras ordinaires que pour l'utilisation de caméras *ANPR*. Dans les deux cas, les images peuvent être conservées pendant 12 mois maximum. En ce qui concerne les missions de police administrative, l'accès est limité au premier mois suivant l'enregistrement des images. Pour les missions de police judiciaire, les images sont accessibles pendant toute la durée de leur conservation mais l'intervention du procureur du Roi est nécessaire après le premier mois[30]. L'accès doit être motivé sur le plan opérationnel et nécessaire pour l'exercice d'une mission précise[31]. Autrement dit, l'accès aux images est autorisé uniquement aux personnes qui ont besoin de ces données à caractère personnel et informations et lorsqu'un intérêt opérationnel concret est donc présent à cet effet[32].

11. En ce qui concerne le droit d'accès aux images de toute personne filmée, le droit à un accès indirect tel qu'il est prévu à l'art. 42 LPD est d'application s'il s'agit d'images traitées à des fins opérationnelles. La LFP ne contient toutefois pas de réglementation relative aux droits du fonctionnaire de police ou du citoyen dans le cadre de l'accès aux images dans l'hypothèse où les images et le son ne sont pas utilisés à des fins opérationnelles (donc, par exemple, lorsqu'elles ne servent pas de base à l'établissement d'un procès-verbal). Si les images ne sont pas pertinentes pour les missions

[24] Voir aussi et plus en détail, Avis d'initiative du COC DD200026 du 11.02.2021 concernant la question de savoir qui est le responsable du traitement pour les traitements de données par les services de police dans le cadre de l'exécution de missions policières d'une part et pour les traitements de données en vertu du RGPD d'autre part, https://www.organedecontrole.be/files/DD200026_Responsable_de_Traitements_GPI_F.PDF
[25] Art. 25/4 § 1, 1° de la LFP.
[26] Exposé des Motifs de cette loi, p. 21 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).
[27] Art. 88 de la loi du 21 mars 2018 et Exposé des Motifs de cette loi, p. 113-114 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).
[28] Art. 25/4 § 2, 2e alinéa de la LFP.
[29] Art. 25/6, 44/11/3*decies* § 2, alinéa premier, et 46/12, alinéa premier de la LFP.
[30] Art. 25/7 § 1, 1er et 2e alinéas et 44/11/3*decies* § 3, deuxième alinéa de la LFP.
[31] Art. 44/11/3*decies* § 3, 1er alinéa de la LFP.
[32] Exposé des Motifs de cette loi, p. 29 (Doc. parl. *Chambre* 2017-2018, n° 54-2855/001).

de police administrative ou judiciaire et n'ont donc pas d'intérêt opérationnel, la LFP ne s'oppose pas non plus à ce que la zone de police responsable organise elle-même un droit d'accès aux images[33]. En l'occurrence, le système d'accès, par analogie à la loi sur les caméras du 21 mars 2007, peut servir d'exemple, le fonctionnaire de police mais aussi le citoyen pouvant ainsi s'adresser directement au service de police concerné.

3.1.6 Utilisation visible et invisible de caméras

12. Les caméras visibles sont les caméras dont l'utilisation est signalée par des pictogrammes, les caméras montées à bord de véhicules de police, de navires de police, d'aéronefs de police, ou de tout autre moyen de transport de police ou portées par des fonctionnaires de police qui sont identifiables comme tels[34]. Dans des situations exceptionnelles, la police peut faire un usage dissimulé de caméras (utilisation non visible). Dans ce cas, la caméra est portée par le fonctionnaire de police ou placée dans un véhicule de police banalisé. Il est question d'un véhicule de police banalisé lorsque le véhicule de police n'est pas reconnaissable en tant que tel. Dans ce cas, il est donc question d'utilisation « *non visible* » de la caméra[35]. L'utilisation de caméras non visibles est régie strictement et se limite à quatre situations. À savoir :
1) en raison de circonstances particulières, notamment en cas d'attroupements, en vue de recueillir des informations de police administrative sur des personnes radicalisées ou *terrorist fighters,* et de véhicules de police banalisées pour la lecture automatique de plaques d'immatriculation, en vue de détecter des véhicules signalés (art. 46/4 LFP) ;
2) pour la préparation d'actions de police judiciaire ou pour le respect de l'ordre public pendant ces actions (articles 46/7 et 46/8 LFP) ;
3) dans le cadre de missions spécialisées de protection des personnes (art. 44/9 LFP) et ;
4) pendant le transfert de personnes détenues ou arrêtées (art. 46/11 LFP).

Sauf si l'utilisation non-visible de caméras est effectuée sous l'autorité d'un magistrat, cette forme d'utilisation de caméras doit toutefois être notifiée **préalablement** à l'Organe de contrôle. Cette notification préalable doit permettre à l'Organe de contrôle d'apprécier la légalité de la décision[36].

3.1.7 Analyse d'impact et de risques et évaluation de l'impact sur la protection des données (EIPD ou *DPIA*, *Data Protection Impact Assessment*)

13. Depuis la loi du 21 mars 2018, il est obligatoire d'établir une analyse d'impact et de risques préalablement à l'utilisation de caméras de surveillance, la protection de la vie privée étant mise en balance avec le niveau opérationnel de l'utilisation des caméras[37]. Cet exercice doit également être établi avant la constitution d'une banque de données technique (locale)[38]. À cet effet, l'assistance du *DPO* est demandée[39].

À condition que les conditions de la LPD pour une *DPIA* et les conditions pour une analyse des risques et d'impact concernant l'utilisation visible des caméras et/ou concernant la constitution des banques de données techniques en vertu de la LFP soient satisfaites, les deux analyses peuvent être réunies en un seul document. Étant donné qu'une *DPIA* en vertu de la LPD nécessite une analyse plus étendue que celle prescrite dans la LFP, il est signalé que, dans le cas où les deux sont traités ensemble, cette analyse doit, conformément à la LPD, couvrir tous les systèmes et procédures pertinents d'opérations de traitement. Hormis le respect de la LPD et de la LFP, les mesures de précaution opérationnelles et les mesures de protection (qui sont prises pour limiter les risques pour les données à caractère personnel à protéger) doivent également être décrites.

3.1.8 Registre

[33] Comme spécifié en principe dans l'article 14 (droit de consultation) de la Directive Police-Justice
[34] Art. 25/2 § 2 de la LFP.
[35] Art. 46/4 et suiv. de la LFP.
[36] Art. 46/6 et 46/10 de la LFP.
[37] Art. 25/4 § 2 de la LFP.
[38] Art. 44/11/3*octies* de la LFP.
[39] Art. 65, 3° *juncto* 58 de la LPD.

14. Les utilisations de caméras doivent être consignées dans un registre (local)[40]. Le registre indique le type de caméras et leur localisation. Cependant, aucun arrêté royal n'a encore été promulgué pour préciser le contenu de ce registre. Néanmoins, l'Organe de contrôle estime qu'à la lumière de l'efficacité de ses compétences de contrôle, la police, en l'attente de l'arrêté d'exécution, doit constituer de sa propre initiative un registre qui reprend toutes les utilisations de (types de) caméras, y compris l'utilisation non-visible de caméras. De cette manière, l'Organe de Contrôle (et, du reste, la zone de police elle-même, en premier ressort) bénéficie d'une vue d'ensemble et a une idée de l'utilisation de caméras de surveillance sur le territoire de la commune qui relève de sa compétence. Dans le même temps, l'utilisation de caméras de surveillance peut être contrôlée en fonction du registre des activités de traitement. Étant donné que des données à caractère personnel sont traitées par la caméra, ce traitement doit également figurer dans le registre des activités de traitement[41]. Les deux registres sont ou doivent être disponibles pour l'Organe de contrôle.

3.1.9 Surveillance par caméras des bâtiments, bureaux de police et cellules de police

15. La surveillance par caméras des bâtiments, bureaux et cellules de police relève de la LFP[42][43]. C'est également le cas de la surveillance par caméras du hall d'entrée ou de l'accueil du commissariat de police. La vidéosurveillance[44] dans les lieux de détention contribue à la protection et à la garantie du bien-être des personnes qui sont privées de leur liberté et contribue par ailleurs à un meilleur respect des droits de la défense, visés à l'article 6 Conv. eur. D.H.[45]. Toutefois, cette vidéosurveillance est imaginable seulement en tant qu'élément ajouté à une série de mesures comme un contrôle physique régulier des personnes détenues, une politique de prévention des suicides, un système efficace de déclaration pour les victimes d'actes illicites dans les cellules, la séparation, l'isolement, l'application de sanctions disciplinaires ou encore la présence d'un avocat pendant l'audition de la police[46]. Le bâtiment de la police – ou le poste de police - doit être équipé d'une signalisation claire de la vidéosurveillance de telle sorte que la personne détenue dans l'une des cellules en soit expressément informée. Les enregistrements de la détention doivent rester complets (aucun effacement partiel ou modification possible) et être conservés pendant une période raisonnable durant laquelle une plainte peut être déposée.

Étant donné que ces images n'ont pas nécessairement, voire généralement pas d'intérêt opérationnel, la procédure pour l'accès indirect à ces images par l'intermédiaire du COC n'est pas d'application et, conformément à la LPD et au RGPD, l'intéressé peut avoir accès directement aux images enregistrées de sa détention.

Lors du visionnage des images des différentes cellules sur les moniteurs dans le commissariat, la police doit prendre plusieurs mesures strictes de sécurité et d'accès : l'accès doit être limité conformément au principe *need to know*. Un accès général aux images (par exemple : moniteurs dans un local de passage des membres du personnel ou à l'accueil) doit être évité.

3.2 Enregistrement audiovisuel dans le cadre d'une instruction pénale

16. En vertu de l'article 112*ter* du Code d'Instruction criminelle (C. I. cr.), « *le procureur du Roi ou le juge d'instruction peut ordonner l'enregistrement audiovisuel ou audio d'une audition. La personne à entendre est préalablement mise au courant de cette décision.* » (§ 1). L'enregistrement audiovisuel ou audio de l'audition peut être effectué par un fonctionnaire de police (§ 2) qui doit dans ce cas reprendre ce mode d'audition dans le procès-verbal (§ 3). Il ne s'agit donc pas d'une forme de surveillance par caméra (avec audio), telle que visée et régie dans la LFP. Par ailleurs, la

[40] Art. 25/8 de la LFP.
[41] Art. 55 de la LPD et 145 LPI.
[42] Voir aussi l'A.R. du 14 septembre 2007 relatif aux normes minimales, à l'implantation et à l'usage des lieux de détention utilisés par les services de police, en particulier l'art. 10.
[43] A l'exception de la surveillance par caméras aux fins de contrôle de l'exécution des conditions de travail (Voir Avis d'initiative de l'Organe de contrôle de l'information policière concernant l'introduction, par la police intégrée, de la surveillance par caméra à des fins de contrôle du respect des conditions de travail, BD200007, 17 août 2020, consultable sur www.organedecontrole.be).
[44] Recommandation 06/11 émanant de l'ancienne Commission de la Protection de la Vie privée ou CPVP – aujourd'hui appelée l'Autorité de Protection des Données ou APD - sur l'installation et l'utilisation de caméras de surveillance dans les lieux de détention (cellules et locaux d'audition) et dans d'autres lieux du commissariat
[45] Convention européenne des Droits de l'Homme
[46] Voir à ce propos : « Les normes du CPT – Chapitres des rapports généraux du CPT consacrés à des questions de fond » (document CPT/Inf/E (2002) 1 – Rev. 2009), disponible sur www.cpt.coe.int/en/docsstandards.htm

décision de procéder à un enregistrement audiovisuel ou audio n'est pas prise à l'initiative du chef de corps. La personne à entendre (et l'avocat) ne peut pas davantage ignorer l'enregistrement audiovisuel ou audio. Un enregistrement audiovisuel dissimulé ou l'utilisation dissimulée de l'enregistrement audiovisuel tel que visé à l'article 112*ter* C. I. Cr. sont donc illégaux.

3.3 Concertation confidentielle avec un avocat

17. Tout cela ressort de la jurisprudence de la Cour européenne des Droits de l'Homme (CEDH)[47]relative à la confidentialité de la relation entre le client et l'avocat. La confidentialité de cette relation[48]est fondamentale et est protégée par les articles 6 et 8 de la Convention européenne des Droits de l'Homme (Conv. Eur. D.H.)[49]. Cette relation touche donc à la fois au droit à la vie privée, au sens large, de l'intéressé (article 8) et à son droit à un procès équitable (article 6).

Nous retrouvons un exemple éloquent d'une affaire dans un commissariat de police dans le cas R.E. c/ Royaume-Uni[50]qui renvoie également à une jurisprudence antérieure : *« 131. The present case concerns the surveillance of legal consultations taking place in a police station, which the Court considers to be analogous to the interception of a telephone call between a lawyer and client. The Court has recognised that, while Article 8 protects the confidentiality of all correspondence between individuals, it will afford* ***"strengthened protection"*** *to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential (Michaud v. France, no. 12323/11, § 118, ECHR 2012). »*

Même la simple présence d'une caméra dans un local destiné à des entretiens confidentiels entre l'avocat et son client peut être contraire aux articles 6 et 8 de la Conv. eur. D.H., indépendamment du fait que celle-ci filme/enregistre effectivement ou non, plus spécifiquement parce que la confidentialité qui devrait pouvoir s'établir pendant un tel entretien n'est pas garantie. *A fortiori* si les images et/ou le son sont effectivement enregistrés ou si l'audio peut être entendu. C'est seulement si l'avocat le demande, dans le cadre de sa sécurité, que l'utilisation de la vidéo et donc **pas** de l'audio peut être justifiée.

4 RESULTATS DU CONTRÔLE

4.1 Enregistrement audiovisuel de la concertation confidentielle

18. Lors de la visite, le COC a pu constater que **:**

1. la surveillance par caméra est utilisée de manière effective au sein du commissariat de police ;
2. la surveillance par caméra est suivie visuellement en temps réel pour les caméras suivantes :
    a. dans le local d'accueil : les cameras à l'extérieur du bâtiment ;
    b. dans le local du dispatching : les caméras des cellules ;
    c. en ce qui concerne les caméras de l'armurerie, le local des pièces à conviction, le local des fouilles et les locaux d'audition/concertation confidentielle : les images ne sont consultables que par le service de contrôle interne et le responsable ICT ;
3. les images des caméras sont conservées pour un délai de maximum 30 jours;
4. les caméras tournent 24/7 sans aucune exception. Par conséquent, les caméras présentes dans les locaux d'audition enregistrent également la concertation confidentielle ;
5. la ZP de l'Arrondissement de Liège utilise des caméras dans les locaux d'audition / de concertation confidentielle de sa propre initiative à des fins de sécurité en général ainsi que pour la sécurité de l'avocat;

[47] Cour européenne des Droits de l'Homme.
[48] Nous renvoyons notamment à CEDH 10 septembre 2013, Helander c/ Finlande, n° 10410/10, et à CEDH 21 février 1975, Golder c/ Royaume-Uni, n° 4451/70.
[49] Convention européenne des Droits de l'Homme.
[50] CEDH R.E. c/ Royaume-Uni du 27 octobre 2015, n° 62498/11.

6. cependant, une utilisation effective de la caméra pendant la concertation confidentielle sous forme d'une surveillance visuelle en temps réel n'intervient pas ;
7. le système d'enregistrement audio tourne 24/7 sans aucune exception dans les locaux d'audition/concertation confidentielle. **Par conséquent, les conversations lors des concertations confidentielles sont également enregistrées** ;
8. cependant, les conversations de la concertation confidentielle ne sont pas écoutées en temps réel ;
9. la ZP de l'Arrondissement de Liège procède à l'enregistrement des conversations dans les locaux d'audition / de concertation confidentielle de sa propre initiative à des fins de sécurité en général ainsi que pour la sécurité de l'avocat;
10. un pictogramme ainsi qu'un texte avertissent les personnes présentes dans les locaux d'audition/concertation confidentielle de l'enregistrement vidéo et audio permanent ;
11. au cours des 5 derniers mois, la zone de police de l'Arrondissement de Liège n'a pas eu des cas dans lesquels des auditions audiovisuelles ont dû être enregistrées à la demande du procureur du Roi / du Juge d'instruction (art. 112ter C.i.cr.) ;
12. cependant, au cas où de telles auditions ont lieu, le même système d'enregistrement audiovisuel sera utilisé ;
13. au vu de l'enregistrement 24/7 dans les locaux d'audition/concertation confidentielle, le déroulement de l'audition est enregistré de manière audiovisuelle après qu'il ait été renoncé à l'assistance d'un avocat (voy. Art. 2bis, §3 loi relative à la détention préventive) ;
14. mis à part une directive (obsolète) datant de 2010, la zone de police de l'Arrondissement de Liège ne dispose pas de directives réglant l'utilisation des caméras à des fins policières. Cependant :
    a. en ce qui concerne les fouilles, celles-ci ont lieu dans le local devant les cellules avec une caméra qui enregistre 24/7. Lorsqu'il s'agit d'une fouille à nu, la pratique consiste à ouvrir la porte de la cellule de manière à empêcher la caméra de surveillance de filmer directement la personne fouillée ;
    b. les accès aux enregistrements des caméras de surveillance et du son sont limités à un seul profil à savoir le profil d'administrateur, qui est uniquement attribué dans les faits à 2 personnes physiques du service ICT sur réquisition du service de contrôle interne ;
    c. le logiciel qui gère les enregistrements des images et du son ne permettant pas un motif de consultation ni une journalisation, les motifs de consultation ainsi que la personne qui a effectué la consultation sont enregistrés dans un carnet de veille ;
    d. un système de back-up n'est pas prévu ;
    e. au cas où le service de contrôle interne aurait besoin des enregistrements, ceux-ci sont exportés sur un disque dur externe. Il n'est pas claire pour le COC dans quelle mesure et comment le contrôle sur le cycle de vie des enregistrements sur ce disque dur est organisé.
15. le COC a pu constater la présence des enregistrements des auditions dans le logiciel qui gère les images des caméras des locaux d'audition/concertation confidentielle. Toutefois, un enregistrement d'une concertation confidentielle n'était pas disponible au sein des images enregistrées. Le COC a pu constater également, que la qualité du son enregistré était faible.

4.2 Enregistrement audiovisuel dans les cellules

19. Le COC a pu constater également l'enregistrement de l'audio en permanence dans les cellules de la zone de police de l'Arrondissement de Liège. Le pictogramme présent dans le complex des cellules, n'en informe pas les personnes arrêtées car uniquement le pictogramme relatif à l'utilisation des caméras est présent. Malgré le fait que la qualité de l'enregistrement du son soit faible, le COC souhaite ici formuler une mise en garde explicite au sujet des articles 314*bis* et 259*bis* du Code pénal, qui protègent le citoyen contre l'écoute, la prise de connaissance et l'enregistrement de *«communications non accessibles au public »*[51]. Cela implique que l'écoute secrète (interception) ou l'enregistrement secret d'une conversation à laquelle on ne prend **pas** part est pénalisé(e) par l'article 314*bis* ou 259*bis* du Code pénal. Le premier article protège la communication dans le chef de particuliers, tandis que le second article offre une protection

[51] Articles 30 à 32 inclus de la loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales. Cette loi a remplacé aux articles 314bis et 259bis du Code pénal le terme *« communications ou télécommunications privées »* par le terme *« communications non accessibles au public »*. Il s'agit d'une modification purement terminologique (Doc. Parl. *Chambre* 2015-2016, n° 54-1966/001, 75). De plus, l'élément *« pendant le transfert »* a été supprimé des deux dispositions pénales.

contre les infractions commises par des fonctionnaires (de police)[52]. Les infractions à la protection des communications ne sont possibles que si – et dans la mesure où – la loi les prévoit, comme dans les circonstances et sous les conditions visées à l'article 90*ter* du Code d'instruction criminelle.

Tant les conversations normales que les télécommunications sont protégées. Il s'agit de communications se déroulant dans la sphère privée[53], étant entendu que le terme 'privé(e)(s)' ne peut pas faire l'objet d'une interprétation restrictive. Toutes les communications sont protégées, même si elles ne touchent pas nécessairement à la vie privée des participants à la conversation. Dès le moment où la conversation n'est pas destinée à être écoutée par des tiers, il s'agit d'une 'communication privée' ou d'une 'communication non accessible au public' au sens de l'article 259*bis* (et de l'article 314*bis*) du Code pénal. En d'autres termes, les conversations menées dans un contexte professionnel sont protégées également[54]. De plus, la protection n'est pas tributaire du lieu mais dépend plutôt du contexte et des intentions des participants à la conversation. Une conversation fait dès lors l'objet de la protection du secret de la communication lorsqu'elle n'est pas destinée à être entendue de tous, où qu'elle ait lieu – dans le salon, sur le lieu de travail ou dans un lieu public[55].

L'article 259*bis* du Code pénal pénalise aussi la prise de connaissance illégale d'une communication à laquelle on ne prend pas part. Or, celui qui enregistre les conversations n'est pas le seul qui en prendra connaissance. Outre le fonctionnaire de police qui enregistre la conversation, la hiérarchie policière aura la plupart du temps elle aussi accès à la communication (les images et le son) (par exemple dans le cadre d'une enquête disciplinaire ou tout simplement à des fins internes de contrôle de qualité).

La protection s'applique uniquement si la conversation est interceptée, est enregistrée ou s'il en est pris connaissance à l'aide d'un appareil quelconque. L'écoute purement sensorielle n'est donc pas répréhensible et ne pose aucun problème, ce qui signifie qu'aucun problème ne se pose lorsque des fonctionnaires de police prennent part activement et/ou passivement (sensoriellement) à la conversation/à l'interaction.

Cela veut toutefois dire que le(s) fonctionnaire(s) de police qui écoute(nt) ou enregistre(nt) la conversation ou qui en prend (prennent) connaissance sans que les conditions de l'article 25/2 §2, 2°, b) de la LFP et de l'article 259*bis* du Code pénal ne soient respectées est (sont) passible(s) de sanctions.

---

[52] L'article 259*bis* du Code pénal est formulé comme suit :
« §1er. Sera puni d'un emprisonnement de six mois à trois ans et d'une amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit :
1° soit, intentionnellement, à l'aide d'un appareil quelconque, intercepte ou fait intercepter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer des communications non accessibles au public, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ;
2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque ;
3° soit, sciemment, détient, révèle ou divulgue à une autre personne le contenu de communications non accessibles au public ou de données d'un système informatique illégalement interceptées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.
§2. Sera puni d'un emprisonnement de six mois à cinq ans et d'une amende de cinq cents euros à trente mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications non accessibles au public ou de données d'un système informatique.
§2bis. Sera puni d'un emprisonnement de six mois à trois ans et d''ne amende de cinq cents euros à vingt mille euros ou d'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au §1er.
§3. La tentative de commettre une des infractions visées aux §§ 1er, 2 ou 2bis est punie comme l'infraction elle-même.
§4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 314bis, §§ 1er à 3. »
[53] La modification de la terminologie ne modifie en rien la portée de la notion de 'communications privées' dans l'ancien article (Doc. Parl. *Chambre* 2015-2016, n° 54-1966/001, 53).
[54] Rapport accompagnant le projet de loi, Doc. Parl. *Sénat* 1992-1993, n° 843/2, 11 (rapport accompagnant le projet de loi).
[55] Rapport accompagnant le projet de loi, Doc. Parl. *Sénat* 1992-1993, n° 843/2, 10 (rapport accompagnant le projet de loi).

Le seul fait que la police soit responsable du bien-être du prévenu ne peut pas être considéré comme une exception explicite à la protection de la communication. La jurisprudence (européenne) a déjà établi à plusieurs reprises qu'une exception à ce droit fondamental doit être prévue de manière claire et explicite (exigence de prévisibilité ;circonstances et conditions dans lesquelles une infraction à la protection des communications est autorisée). Le seul fait qu'il se retrouve dans une cellule de police et relève ainsi de la responsabilité de la police ne justifie par exemple pas que l'on puisse enregistrer un monologue du prévenu sans son consentement.

Comme le défend le COC dans son avis sur les *bodycams*[56], la police peut dans certaines situations être considérée comme un 'participant' à la communication. De l'avis du COC, cela peut en l'occurrence être le cas lorsque le fonctionnaire de police utilise l'intercom pour savoir comment se porte le prévenu et enregistre ce faisant la communication. À l'inverse, cela peut également être le cas lorsque le prévenu contacte le fonctionnaire de police au moyen de l'intercom/du bouton d'urgence. Il n'est pas sans importance d'en informer le prévenu au préalable. Par contre, l'enregistrement systématique de la communication du prévenu constituera selon toute probabilité une infraction à l'article 259*bis* du Code pénal, précisément parce que la police ne peut pas être automatiquement considérée comme un participant à la conversation. Un avertissement général affiché dans le complexe de cellules ne sera pas non plus assimilé à un consentement (implicite) du prévenu.

5 CONCLUSIONS, DEMANDES ET MESURES CORRECTRICES

20. Des réponses obtenues, le COC a pu constater clairement que la zone de police de l'Arrondissement de Liège enregistre en permanence les images et le son relatives à la concertation confidentielle, sans nécessairement en informer explicitement l'avocat et son client. Un pictogramme ainsi qu'un texte informent l'avocat et son client de cet enregistrement en permanence.

21. Le COC a également pu constater l'enregistrement audiovisuel en permanence dans les cellules. Cependant, les personnes arrêtées ne sont pas informées de l'enregistrement du son en permanence.

22. Il n'y a pas de directives disponibles par rapport à ce traitement.

23. L'accès aux images et au son enregistrées est limité à deux personnes qui partagent le même compte.

24. Le logiciel qui gère les images et le son ne permet ni l'enregistrement d'un motif de consultation, ni une journalisation. Ce défaut technique est atténué sous forme d'une mesure organisationelle à savoir l'enregistrement des motifs de consultations dans un cahier de veille.

25. Il n'y a pas de *back-up*. Il n'est pas claire comment le traitement ultérieure via disque dur est organisé.

PAR CES MOTIFS,

L'Organe de Contrôle ;

demande la zone de police de l'Arrondissement de Liège,

1. Demande

[56] Avis d'initiative de l'Organe de contrôle de l'information policière suite aux constatations dans le cadre d'une enquête sur l'utilisation de *bodycams*, 8 mai 2020, CON19008.

d'adopter des directives claires en matière d'utilisation de caméras dans la zone de police en général et dans le bâtiment de police en particulier. Ces directives doivent au moins tenir compte des profils, compléter le motif de la consultation, les délais d'enregistrement, les fichiers de journalisation et le traitement ultérieur des enregistrements le cas échéant;

2. Demande

d'étudier la possibilité de prévoir un local séparé dans lequel la concertation confidentielle entre l'avocat et son client pourrait avoir lieu ;

3. Demande

d'étudier la possibilité d'équiper le système d'enregistrement des images et du son dans les locaux d'audition d'un bouton marche-arrêt clairement visible permettant d'activer et de désactiver le système de caméras ;

4. Demande

de bien vouloir communiquer avant l'audition les motifs ainsi que les modalités de l'utilisation des caméras à l'avocat et à son client, et d'en faire acte dans le procès-verbal.

* * * * * * * * *

Vu les articles 221 § 1 et 247, 4°, 5° et 6° LPD,

Ordonne les mesures correctrices suivantes à la zone de police de l'Arrondissement de Liège,

a. Mesure correctrice a)

Vu les constations reprises au point 18, à savoir l'enregistrement en permanence de la concertation confidentielle entre l'avocat et son client, **à effet immédiat** mettre fin à la prise d'images et l'enregistrement audio en permanence de la concertation confidentielle entre l'avocat et son client et en donner confirmation à l'Organe de contrôle ; dit pour droit qu'il faut entendre par *« effet immédiat »* la date de la transmission du présent rapport (par e-mail) par l'Organe de contrôle majorée de deux jours ouvrables (samedi et dimanche non inclus) ;

b. Mesure correctrice b)

Vu les constatations reprises au point 19, à savoir l'enregistrement en permanence du son dans les cellules donnant la possibilité d'intercepter ou d'écouter secrètement les conversations ;

le COC ordonne à la zone de police de l'Arrondissement de Liège de mettre les enregistrements sonores dans les cellules en conformité avec le cadre légal en vigueur sur le plan de la collecte, de la conservation, de l'accès et de la journalisation, et **ce dans les six mois** à compter de la réception du présent rapport ; dit pour droit qu'il faut entendre par *« dans les six mois »* la date de la transmission du présent rapport (par e-mail) par l'Organe de contrôle majorée de deux jours ouvrables (samedi et dimanche non inclus)

Ainsi décidé par l'Organe de contrôle de l'information policière le 29 mars 2022.

Pour l'Organe de contrôle,

Koen Gorissen Membre-conseiller	Frank Schuermans Membre-conseiller	Philippe Arnould Président

Copie :

- Le président du collège de police
- Le procureur du Roi de Liège

Controleorgaan op de politionele informatie

Organe de contrôle de l'information policière