DSJ/ janvier 2019

Rapport explicatif accompagnant l'avant-projet de loi modifiant la loi sur la Police cantonale

Le présent rapport explicatif se divise selon le plan suivant :

1 ORIGINE ET NÉCESSITÉ DU PROJET

La loi du 15 novembre 1990 sur la Police cantonale (LPol ; RSF 551.1) a connu plusieurs modifications depuis son adoption il y a bientôt 30 ans. La dernière révision en date remonte à 2013 (mesures d'investigation secrète).

Dans les grandes lignes, la présente révision de la loi sur la police cantonale se conçoit sous quatre aspects (dans l'ordre d'importance).

Premièrement, une nouveauté est introduite. Il s'agit d'un concept de gestion des menaces visant à prévenir des actes de violence de personnes dites à risques, par la détection précoce, la collaboration interdisciplinaire et la collecte et l'échange de données. Outre la nécessité d'un tel concept, afin de prévenir des risques toujours plus prégnants de commission d'actes de violence, le concept de gestion des menaces est également une mesure recommandée par le Plan d'action national de lutte contre la radicalisation et l'extrémisme violent (PAN). Ce concept de gestion des menaces constitue également un axe de la politique de lutte contre la criminalité 2018-2021 arrêtée conjointement par le Procureur général et le Conseil d'Etat, en vertu de l'article 67 al. 3 let. c de la loi du 31 mai 2010 sur la justice (LJ ; RSF 130.1).

Deuxièmement, afin de combler une lacune juridique cantonale découlant de la mise en œuvre du Système d'Information Schengen II (SIS II), il est proposé d'introduire, dans la LPol, une nouvelle base légale applicable aux signalements selon l'art. 36 de la décision 2007/533/JAI du Conseil de l'Union européenne du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II).

Troisièmement, la nouvelle loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; RS 780.1) prévoit deux bases légales réglant la recherche de personnes disparues et la recherche de personnes condamnées. Il convient dès lors d'adapter la législation cantonale afin de supprimer un conflit de norme, respectivement régler la compétence des autorités cantonales en la matière.

Enfin, il est apparu que certaines dispositions de la LPol étaient devenues obsolètes du point de vue de l'organisation et de l'évolution des activités de la Police cantonale, raison pour laquelle il est proposé de procéder, en plus des modifications substantielles précédemment mentionnées, à des modifications mineures de la LPol afin d'assurer une cohérence systématique et une cohérence opérationnelle.

2 INTRODUCTION D'UN CONCEPT DE GESTION DES MENACES

La gestion des menaces s'inscrit dans le cadre des tâches régaliennes de l'Etat d'assurer la sécurité de ses citoyen-ne-s et de prévenir les risques, grâce au travail de police. De manière schématique, le travail policier peut être appréhendé sous deux aspects.

D'une part, le travail *réactif* qui consiste à réagir aux phénomènes criminogènes et aux troubles à l'ordre public par un travail d'enquête policière et d'investigations scientifiques ou par des moyens d'intervention répressifs. Ce travail réactif se situe, bien souvent, dans le cadre de la procédure pénale (procédure préliminaire, art. 299ss du Code de procédure pénale, CPP ; RS 312.0). L'ouverture d'une procédure pénale présuppose l'existence d'un soupçon initial suffisant qu'une infraction pénale ait été commise.

D'autre part, le travail *préventif* qui vise à prévenir les phénomènes criminogènes et les troubles à l'ordre public, par un travail de recherche d'informations et de renseignements (investigations préliminaires) dont l'assise légale se trouve dans le droit cantonal de police (art. 33a – observation préventive, 33b – recherches préventives secrètes et 33c – investigation préventive secrète – LPol) ainsi que dans la loi fédérale sur le renseignement (LRens ; RS 121).

La gestion des menaces s'inscrit dans le champ d'action préventif du travail policier mais se situe le plus souvent en dehors de la procédure pénale, sans toutefois l'exclure totalement, les deux aspects étant parfois intrinsèquement liés (ex. commission d'infractions antérieure aux menaces actuelles). La gestion des menaces nécessite dès lors des dispositions légales spécifiques englobant une réalité sécuritaire tout à fait spécifique.

2.1 Nécessité du projet

Un certain nombre de drames se sont produits au cours des dernières années en Suisse (ex. tuerie au Parlement de Zoug en 2001, parricide de Pfäffikon en 2015, attaque à la hache à Flums en 2017) comme à l'étranger (ex. attaque au moyen d'un véhicule à Münster, Allemagne en mai 2018). Le canton de Fribourg n'a pas été épargné, en témoigne par exemple le saccage du service social de la commune de Romont en janvier 2017. Les personnes ayant commis ces actes de violence étaient connues des services de l'Etat, mais l'échange d'informations s'était heurté à un manque d'organisation et/ou aux règles strictes en matière de protection des données et de secret professionnel.

La nécessité d'une gestion des menaces se situe à deux niveaux. Premièrement et sous l'angle sécuritaire, afin de protéger des tiers de la commission d'infractions graves et paraissant inéluctables à leur encontre. Deuxièmement et sous l'angle social, afin d'offrir une issue favorable, par des mesures de soutien, à des personnes en proie à une forme de désespoir ou vivant une situation personnelle tourmentée les amenant à envisager des actes de violence.

Il convient également de relever l'importance de la gestion des menaces dans deux cas spécifiques : la lutte contre la violence domestique et la lutte contre la radicalisation et l'extrémisme violent. Dans les situations de violence domestique, les spécialistes appelé-e-s à intervenir au long de la procédure sont divers (police, Ministère public, centres de consultation d'aide aux victimes, médecins, psychologues, service de l'enfance et de la jeunesse). Un concept de gestion des menaces permet d'atteindre une politique de lutte contre la violence domestique plus efficiente et de réduire le risque de passage à l'acte ou de récidive, par une action globale et immédiate et par la communication interinstitutionnelle d'informations. Les cantons qui appliquent déjà un concept de gestion des menaces relatent que dans 50 % des cas, les alertes données dans le cadre de la gestion des menaces concernent des situations de violences domestiques. A cet égard, il convient de relever que le concept d'action « *Violence au sein du couple et ses impacts sur la famille* » du Conseil d'Etat pour le canton de Fribourg[1] met en exergue la gestion coordonnée des menaces comme prioritaire et urgente.

[1] Disponible à cette adresse : https://www.fr.ch/sites/default/files/2018-08/concept_violence_au_sein_du_couple_conseil_detat_juin_18.pdf (consulté le 6 décembre 2018).

Enfin, le plan d'action national de lutte contre la radicalisation et l'extrémisme violent (PAN[2]) recommande la mise en place et l'introduction d'un concept de gestion des menaces (mesure 14), en y incluant la problématique de la radicalisation et de l'extrémisme violent.

2.2 Définition et but de la gestion des menaces

La gestion des menaces peut être définie comme le processus standardisé visant à empêcher des personnes présentant un potentiel de dangerosité (« personnes à risques ») de commettre des actes graves et ciblés de violence contre des tiers, moyennant l'implication d'un réseau interdisciplinaire de spécialistes et d'interlocuteurs et interlocutrices du terrain. La gestion des menaces s'appuie sur l'analyse précoce de certains comportements laissant indiquer un risque accru de commission d'actes de violence.

La gestion des menaces est un processus interdisciplinaire préventif accompagnant individuellement chaque cas particulier (« gestion de cas » ou « case management », en anglais), en présence de risques factuels et tangibles. Une gestion des menaces durable telle que conçue dans le présent projet nécessite la présence d'une unité fixe au sein de la Police. Cette unité doit être soutenue par des spécialistes issus en particulier des domaines de la santé mentale, des préfectures et des justices de paix et accompagnée d'un réseau au sein de tous les échelons publics et privés concernés (cf. détail de la structure du projet au chapitre 2.5). La gestion des menaces prévoit donc une approche préventive, mais aussi une approche orientée vers des solutions pour les personnes à risques, le but étant que la personne retrouve pied et sorte durablement de sa situation personnelle troublée.

Les cas d'application typiques de la gestion des menaces concernent notamment les violences domestiques, le harcèlement obsessionnel (stalking), les menaces substantielles, qu'elles soient ouvertes, cachées, anonymes ou identifiées, les comportements quérulents, les comportements violents liés à des troubles mentaux ou encore le harcèlement sexuel.

Dans ce contexte, une attention particulière est donnée à la protection des victimes. Ainsi, la sécurité et l'intégrité physique, psychique et sexuelle des victimes potentielles doit être assurée en visant à trouver une solution pour la personne représentant un danger et de ce fait empêcher durablement le passage à l'acte.

Enfin, la gestion des menaces permet d'offrir un cadre d'écoute aux services de l'Etat, des communes et d'autres institutions qui font régulièrement l'objet de menaces dans le cadre de leur activité. Il convient à cet égard de rappeler que certains services publics et leurs employé-e-s font quotidiennement l'objet de menaces de la part de personnes ; il convient dès lors d'offrir un soutien et un appui à ces services dans l'appréciation du risque.

2.3 Situation actuelle : faiblesse du cadre légal pour une collaboration interdisciplinaire

A l'heure actuelle, dans le canton de Fribourg, aucune collaboration interdisciplinaire et aucun échange d'informations entre les services des administrations publiques cantonale et communale ne sont formalisés. Il n'existe pas de processus standardisé d'annonce et de suivi des cas, alors que de nombreux services de l'Etat et des communes sont confrontés régulièrement à de telles personnes à risques. Le constat est clair : chaque service dispose potentiellement d'informations préoccupantes liées à des personnes à risques mais en l'absence de recoupement de ces informations, le risque ne peut précisément pas être évalué. Dans les exemples mentionnés plus haut (cf. chapitre 2.1), l'analyse des cas *a posteriori* a permis de constater que chaque service et chaque acteur concernés

[2] Disponible à cette adresse : https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2017/2017-12-04/171204-nap-f.pdf (consulté le 6 décembre 2018).

disposaient d'une partie de l'information liée à la dangerosité de l'auteur d'actes de violence, mais l'absence de collaboration et d'échange d'informations a empêché de procéder à une évaluation du risque. Celui-ci s'est donc réalisé alors qu'il aurait sans doute pu être évité si ces cas avait fait l'objet d'un monitorage et d'une collaboration interdisciplinaire.

Or, la collaboration interdisciplinaire nécessite une base légale qui en règle le principe et fixe le processus d'annonce des cas, en particulier en ce qui concerne le déliement du secret professionnel. Il s'agit en outre de prévoir des règles spécifiques concernant la collecte et l'échange de données entre les partenaires concernés par la gestion des menaces (cf. ci-dessous, chapitres 2.3.1 et 2.3.2).

Les développements ci-dessous démontrent la faiblesse d'un système actuel fait de règles disparates, régissant la menace et le risque sous des angles spécifiques et essentiellement réactifs, alors que la gestion des menaces nécessite une approche globale et préventive.

2.3.1 Echange de données

La collaboration interdisciplinaire dans le cadre de la gestion des menaces nécessite une collecte et une transmission de données personnelles qui peuvent être considérées comme sensibles. En effet, au sens de l'article 3 al. 1 de la loi du 25 novembre 1994 sur la protection des données (LPrD, RSF 17.1) les données sensibles sont des données personnelles se rapportant aux opinions ou activités religieuses, philosophiques, politiques ou syndicales, à la santé, la sphère intime ou l'appartenance à une race, à des mesures d'aide sociale ou à des sanctions pénales ou administratives et les procédures y relatives. Dans le cadre de la gestion des menaces, il est prévisible que de telles données sensibles soient présentes dans les informations collectées.

L'article 9 LPrD règle la collecte de données. En principe, les informations doivent être recueillies directement auprès de la personne concernée. Elles peuvent être collectées auprès d'organes publics ou de tiers que si une disposition légale le prévoit, si la nature de la tâche l'exige ou si des circonstances particulières le justifient.

L'article 10 LPrD permet la communication de données personnelles en l'existence d'une base légale ou si, dans le cas d'espèce :

a) l'organe public qui demande les données en a besoin pour l'accomplissement de sa tâche ;

b) la personne privée qui demande les données justifie d'un intérêt à la communication primant celui de la personne concernée à ce que les données ne soient pas communiquées, ou que

c) la personne concernée a consenti à la communication, ou les circonstances permettent de présumer un tel consentement.

Le droit cantonal ne prévoit actuellement pas de base légale autorisant la collecte et l'échange de données dans le cadre d'une collaboration interdisciplinaire de gestion des menaces. Les trois conditions alternatives prévues par la LPrD doivent être examinées au cas par cas, en retenant que la troisième condition (let. c) n'est pas applicable, au regard du fait que la personne à risque ne doit pas être informée de la collecte et l'échange de données la concernant, en tout cas dans la phase d'identification et d'évaluation du risque.

Reste enfin réservée la clause générale d'urgence, permettant la restriction d'un droit fondamental en cas de danger sérieux, direct et imminent (art. 38 Constitution du canton de Fribourg, RSF 10.1 ; art. 36 Constitution fédérale, RS 101). Cette clause d'urgence n'est toutefois qu'une solution réactive et qui n'a qu'une portée mineure dans le cadre de la gestion des menaces, étant entendu que cette dernière nécessite une collecte et un échange de données en amont d'une éventuelle réalisation du risque.

Au regard de la sensibilité des données qui doivent être traitées dans le cadre de la gestion de menaces et des atteintes nécessaires aux droits fondamentaux des personnes à risques, une base légale de rang formel est indispensable, afin de légitimer l'action de toutes les personnes intervenant dans le cadre de la gestion des menaces et garantir une utilisation licite et proportionnée des données.

2.3.2 Secret de fonction et secret professionnel

L'article 320 du Code pénal (CP, RS 311.0) punit celui ou celle qui aura révélé un secret à lui confié en sa qualité de membre d'une autorité ou de fonctionnaire, ou dont il avait eu connaissance à raison de sa charge ou de son emploi.

L'article 321 CP réprime la violation du secret professionnel par les ecclésiastiques, avocats, défenseurs en justice, notaires, conseils en brevet, contrôleurs astreints au secret professionnel en vertu du code des obligations, médecins, dentistes, chiropraticiens, pharmaciens, sages-femmes, psychologues, ainsi que leurs auxiliaires.

La punissabilité est exclue si la révélation du secret est faite avec le consentement de l'intéressé-e ou si l'autorité supérieure ou l'autorité de surveillance l'a autorisée par écrit (art. 320 al. 2 et 321 al. 2 CP). L'état de nécessité (art. 17 CP) permet également d'exclure la punissabilité de quiconque commettant un acte punissable pour préserver d'un danger imminent et impossible à détourner autrement un bien juridique lui appartenant ou appartenant à un tiers.

Enfin, tant le droit fédéral que le droit cantonal prévoient des obligations et des droits d'annonce, comme par exemple l'article 364 CP (droit d'aviser l'autorité de protection de l'enfance en cas de suspicion de maltraitance), les articles 73 et 119 de la loi sur la santé (LSan, RSF 821.0.1 ; obligation d'annonce aux autorités compétentes pour procéder à une levée de corps en cas de mort suspecte et obligation d'annonce en cas de maladie transmissibles à déclaration obligatoire) et l'article 3c de la loi fédérale sur les stupéfiants (LStup, RS 812.121 ; droit d'annoncer aux institutions de traitement ou aux services d'aide sociale compétents les cas de personnes souffrant de troubles liés à l'addiction ou présentant des risques de troubles).

Comme pour l'échange de données en vertu de la LPrD, une gestion des menaces selon un principe d'anticipation des risques exclut le consentement de la personne à risques. Le secret professionnel (secret médical) des professionnel-le-s de la santé est le principal écueil actuellement rencontré dans la volonté de recueillir et d'échanger des informations de manière interdisciplinaire dans le cadre d'une gestion des menaces efficiente. En effet, la crainte, par les professionnel-le-s de la santé, de faire l'objet de poursuites pénales est un obstacle important dans la communication d'informations en lien avec des personnes à risques.

Dans ce contexte, la création d'une base légale spécifique permet aux professionnel-le-s de la santé et aux fonctionnaires de collaborer sans risques de poursuite pénale ultérieure.

2.3.3 Révélation de données dans le cadre d'une procédure pénale

L'article 73 du Code de procédure pénale (CPP, RS 312.0) dispose que : « *les membres des autorités pénales, leurs collaborateurs, ainsi que leurs experts commis d'office gardent le silence sur les faits qui parviennent à leur connaissance dans l'exercice de leur activité officielle* ».

L'article 75 CPP prévoit plusieurs exceptions : information des services sociaux et des autorités tutélaires (al. 2), informations aux autorités tutélaires en cas d'infractions impliquant des mineur-e-s (al. 3) et information au Groupement défense (Armée suisse) en cas de signes ou indices sérieux qu'un militaire ou un conscrit pourraient utiliser une arme à feu d'une manière dangereuse pour eux-mêmes ou pour autrui (al. 3bis).

L'écueil ici constaté consiste dans le fait que les cas relevant de la gestion des menaces se situent bien souvent en dehors d'une procédure pénale. Les règles du CPP ne trouvent dès lors application que de manière marginale dans le cadre de la gestion des menaces.

2.3.4 Autres bases légales

Différentes bases légales permettent (mais n'obligent pas) d'annoncer certains faits aux autorités compétentes.

Premièrement, le Code civil suisse (CC, RS 210) prévoit, dans le cadre des règles de protection de l'adulte et de l'enfant, un certain nombre de dispositions autorisant un avis à l'autorité de protection de l'adulte et de l'enfant.

- Art. 443 al. 1 CC : avis si une personne ou un enfant semble avoir besoin d'aide ;
- Art. 453 al. 2 CC : autorisation d'être délié du secret de fonction ou du secret professionnel et d'aviser s'il existe un danger réel qu'une personne ayant besoin d'aide commette un crime ou un délit qui cause un grave dommage corporel, moral ou matériel à autrui ;
- Art. 443 al. 2 CC : Obligation d'avis, dans l'exercice de fonctions officielles, si une personne ou un enfant a besoin d'aide.

Deuxièmement, la Loi fédérale sur l'aide aux victimes d'infractions (LAVI, RS 312.5) prévoit que l'obligation de garder le secret peut être levée si la victime consent à la transmission d'informations à d'autres services en cas de situation de mise en danger. L'article 11 al. 3 LAVI dispose que : « *si l'intégrité physique, psychique ou sexuelle d'une victime mineure ou d'un autre mineur est sérieusement mise en danger, les personnes travaillant pour un centre de consultation peuvent en aviser l'autorité tutélaire et dénoncer l'infraction à l'autorité de poursuite pénale* ».

Troisièmement, la Loi fédérale sur les armes (LArm ; RS 514.54) autorise les personnes astreintes au secret de fonction ou au secret professionnel de communiquer aux autorités cantonales et fédérales de police et de justices compétentes l'identité des personnes qui mettent en danger leur propre personne ou autrui par l'utilisation d'armes ou qui menacent d'utiliser des armes contre leur propre personne ou contre autrui.

Enfin, il convient de rappeler l'article 17 CP (état de nécessité licite) qui prévoit que : « *quiconque commet un acte punissable pour préserver d'un danger imminent et impossible à détourner autrement un bien juridique lui appartenant ou appartenant à un tiers agit de manière licite s'il sauvegarde ainsi des intérêts prépondérants* ».

2.4 Droit comparé

Plusieurs cantons se sont dotés, à satisfaction, d'un concept de gestion des menaces. Les cantons de Neuchâtel, Bâle-Campagne, Soleure, Glaris, Lucerne, Schwyz, Thurgovie, Saint-Gall et Zurich travaillent déjà avec la gestion des menaces. Les autres cantons romands, de Bâle-ville et du Tessin étudient actuellement la mise sur pied d'un concept de gestion des menaces[3].

Deux exemples sont présentés ici, les cantons de Zurich et Bâle-Campagne.

2.4.1 Zurich

Le canton de Zurich est régulièrement cité comme un modèle dans le domaine de la gestion des menaces. Son approche globale de gestion des menaces prévoit un-e interlocuteur/trice dans chaque

[3] S'agissant du canton du Tessin, le concept est mis en place, les démarches en cours consistent à formaliser le concept par une base légale.

office, chaque service et chaque institution du canton. En cas de besoin, les interlocuteurs/trices transmettent des informations à la police, chargée de la direction des opérations. L'appui du centre *Forensic Assesment & Risk Management*, disposant de compétences en matière de psychiatrie forensique, peut être requis pour procéder à une évaluation approfondie de la dangerosité et apprécier les modes d'intervention pour le cas particulier. En outre, un groupe interdisciplinaire d'expert-e-s peut être réuni pour définir des mesures propres à désamorcer la violence.

2.4.2 Bâle-Campagne

Le canton de Bâle-Campagne dispose d'un concept global de gestion des menaces. Les cas peuvent être annoncés par une série d'institutions et d'entités auprès du service de la gestion des menaces, rattaché au Secrétariat général du Département de la sécurité. Le service de la gestion des menaces procède à une évaluation et classe les cas selon cinq catégories de risques. Lorsque les cas sont jugés avec un risque accru ou élevé, une équipe de spécialistes est réunie. Le service de gestion des menaces procède au suivi du cas et observe la dynamique du risque en mettant ses données régulièrement à jour. Au besoin, un monitorage du cas est mis en place, pour un suivi resserré.

2.5 Système proposé

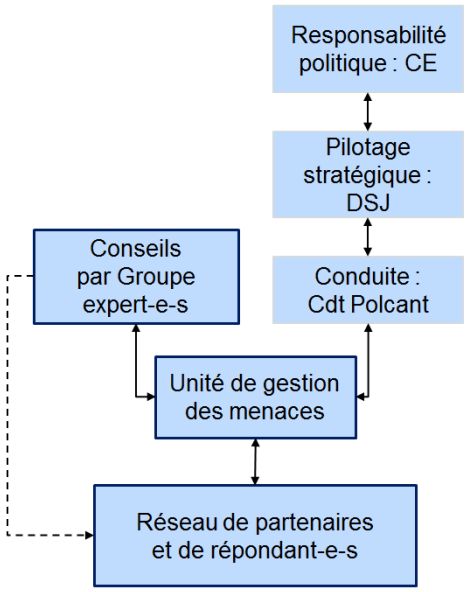
Le système développé dans le présent projet repose sur une approche globale de la gestion des menaces, incluant toute forme de risques de violences reposant sur des menaces sérieuses (mais pas forcément imminentes) à l'encontre de tiers. Ce système global se justifie afin d'offrir une garantie contre le risque la plus haute possible et d'appréhender le risque de manière uniforme et transversale. Le système proposé se base sur une analyse des concepts de gestion des menaces des autres cantons et est adapté à l'environnement institutionnel fribourgeois.

2.5.1 Organisation (ad articles 30g, 30h et 30i de l'avant-projet)

La gestion des menaces ne peut pas être appréhendée comme une thématique purement policière. La prévention des actes de violence incombe à de nombreux services et institutions évoluant au contact des citoyen-ne-s. L'on pense aux autorités de protection de l'adulte et de l'enfant, aux milieux médicaux, à bon nombre de services de l'Etat (services des impôts, offices des poursuites et des faillites, préfectures, etc…), aux autorités judiciaires ainsi qu'aux services des administrations communales et aux organismes de soutien aux personnes (ex. centres LAVI, fondations et associations oeuvrant dans les domaines social et médico-social, dans le soutien aux adultes, enfants et aux familles, dans le soutien aux personnes toxicomanes ou dépendantes).

Le risque est un élément dynamique en perpétuel changement. Ce risque, tel que conçu dans la gestion des menaces, diffère de l'évaluation du risque en psychiatrie forensique. Ainsi, une démarche concertée et l'usage d'outils d'évaluation et d'une approche par gradation sont nécessaires.

Les grandes lignes de l'organisation du concept de gestion des menaces peuvent être schématisées de la manière suivante :



Ci-après l'organisation est présentée de manière détaillée.

Unité de gestion des menaces (art. 30g)

L'unité de gestion des menaces (ci-après : UGM) est le centre opérationnel de la gestion des menaces. Elle est l'unité répondante chargée de recevoir les annonces de cas. Reconnaître, évaluer, désamorcer sont les trois mots-clés régissant l'activité de l'UGM.

L'UGM est ainsi chargée :

- d'enregistrer les annonces de cas par les membres du réseau et procéder à une première évaluation du risque ;
- d'examiner la typicité des cas annoncés et d'en assurer le suivi, avec le soutien régulier du groupe d'expert-e-s et en collaboration avec les partenaires concernés du réseau (cf. ci-après « groupe d'expert-e-s ») ;
- de tenir à jour la base de données des cas annoncés et suivis ;
- de prendre les mesures nécessaires et idoines au sens de l'article 30j de l'avant-projet (cf. chapitre 2.5.2) ;
- de former et de maintenir le réseau des partenaires et de coordonner l'action des répondant-e-s ;
- d'assurer la formation initiale et continue des répondant-e-s du réseau ;

L'UGM doit être créée au sein du Commandement de la Police cantonale et devrait être constituée de trois EPT : deux policiers/ères déjà issus du corps de police et un-e collaborateur/rice scientifique (idéalement un-e psychologue/criminologue).

Les policiers/ères engagés dans l'unité devront réunir un certain nombre de compétences, telles que connaissances de la gestion des risques, expérience du travail de désarmorçage, capacités d'empathie supérieures, résistance au stress psychologique, capacité de persuasion et compétences en communication.

La présence d'un-e psychologue/criminologue dans l'UGM est indispensable, afin de faire bénéficier l'unité de connaissances spécialisées et d'une expérience civile externe au travail policier. Cela permettra également à l'unité de disposer d'une personne compétente pour dispenser les formations nécessaires aux répondant-e-s.

Groupe d'expert-e-s (art. 30h)

Outre l'évaluation quotidienne des cas, il est important que l'UGM puisse s'appuyer sur le soutien et le jugement de spécialistes de la psychiatrie et de la psychologie forensiques, de la santé mentale, du domaine policier, de représentant-e-s des préfectures et des justices de paix par exemples. En effet, le suivi des cas nécessite des prises de décisions concertées et un appui à la décision.

Ainsi, il est prévu que l'UGM puisse convoquer certain-e-s membres du groupe d'expert-e-s régulièrement, afin de discuter des cas appelant par exemple un questionnement sur la dangerosité ou sur la typicité de la menace. Cela permettra à l'UGM de s'appuyer sur l'analyse de ces expert-e-s pour décider de mesures adaptées et de l'angle d'action approprié, au vu des spécificités de la personne à risques et de son parcours de vie.

Ce groupe d'expert-e-s est conçu comme un gremium de personnes ressources dont le soutien peut être sollicité régulièrement, lorsque l'évaluation des cas est complexe.

Réseau d'annonce et partenariat (art. 30i)

La question de l'annonce dans la gestion de la menace est un point central et fondamental du concept de gestion des menaces. Il est en effet essentiel que les informations remontent auprès de l'UGM et que l'UGM fasse redescendre certaines informations auprès des partenaires concernés, afin que la menace soit évaluée et traitée. Ainsi lorsque des menaces entrant dans le champ d'application de la LPol surviennent, les personnes répondantes auprès des partenaires avisent l'UGM. Il convient de préciser d'emblée que l'anonymat est garanti dans le contexte de l'annonce de telle sorte que la personne à risques ne sera pas informée du nom de la personne, de l'autorité ou du partenaire institutionnel ou privé ayant annoncé le cas, sauf à supposer qu'il s'agisse d'un acte de dénonciation calomnieuse au sens de l'article 303 CP.

Dans la mesure où il est prévisible que les cas de personnes à risques seront détectés par des professionnel-le-s de la santé (en particulier psychiatres, psychologues et services médicaux de premier recours) ou des fonctionnaires, il est important de donner à ces personnes une base légale spécifique les déliant de leur secret professionnel et de leur secret de fonction et ceci afin de leur éviter toute sanction pénale selon les articles 320 et 321 CP (cf. également ci-dessus, chapitre 2.3.2). Il convient encore de relever que la levée du secret professionnel concerne également les ecclésiastiques et leurs auxiliaires et que la notion d'ecclésiastiques inclut les évêques, les prêtres et les pasteur-e-s des communautés chrétiennes, mais aussi les prédicateurs des autres religions, tels que les rabbins, imams et chefs bouddhistes[4].

Initialement envisagée, l'obligation d'annonce par les professionnel-le-s de la santé n'a pas été retenue pour deux raisons. Premièrement, il existe un risque qu'une obligation d'annonce nuise à la relation de confiance entre le/la thérapeute et la personne à risques, cette dernière évitant de se livrer totalement à son/sa thérapeute ou renonçant à consulter, de peur de voir son cas annoncé à l'UGM. Deuxièmement, il faut relever que l'obligation d'annonce est difficilement applicable et par là, punissable, en raison du manque de contrôle possible quant aux informations éventuellement retenues par les professionnel-le-s de la santé.

Aussi, la mise en œuvre du concept de gestion des menaces impliquera une forte sensibilisation des milieux médicaux afin que ces derniers, sur une base volontaire, saisissent l'importance sécuritaire et sociale du système d'annonce et conçoivent cette annonce comme une partie de leur responsabilité professionnelle et éthique.

[4] Cf. DUPUIS Michel et al., *Petit commentaire du Code pénal (PC CP)*, p. 2023, Bâle, 2017.

L'UGM sera chargée de constituer le réseau des partenaires qui devra être conçu comme une collaboration dynamique et évolutive, tant ascendante que descendante. Si le réseau des partenaires devra être affiné lors de la mise en œuvre opérationnelle, on peut d'ores et déjà partir du principe que les services publics suivants seront concernés :

- Police cantonale, notamment la police mobile, la police de proximité et la police de sûreté ;
- Pouvoir judiciaire, notamment le Ministère public, les justices de paix et les offices des poursuites et des faillites ;
- Acteurs de la santé publique, notamment l'Hôpital fribourgeois (HFR), le Réseau fribourgeois de santé mentale (RFSM) et le Centre fribourgeois de santé sexuelle ;
- Centres d'aide aux victimes ;
- Service de l'enfance et de la jeunesse ;
- Autorités scolaires, degrés primaires et secondaires (I et II), incluant également le service auxiliaire scolaire, les services de médecine et de psychologie scolaire ;
- Hautes écoles et Université ;
- Communes, notamment les polices locales, les services des curatelles et les services d'aide sociale ;
- Administrations fiscales (cantonale et communales) ;
- Offices régionaux de placement ;
- Bureau de l'égalité et de la famille, notamment la Commission contre la violence au sein du couple et ses impacts sur la famille ;
- Acteurs de l'exécution des peines (Service de l'exécution des sanctions pénales et de la probation et Etablissement de détention fribourgeois) ;
- Préfectures ;
- Service de la population et des migrants ;
- Service des affaires institutionnelles, des naturalisations et de l'état civil ;
- Service de la sécurité alimentaire et des affaires vétérinaires ;
- Médiation administrative cantonale.

Quant aux partenaires institutionnels publics et privés, une première projection permet de considérer les partenaires suivants comme incontournables au réseau :

- Acteurs de la santé privée, notamment médecins de premier recours, psychiatres et psychologues ;
- Corporations religieuses reconnues et associations religieuses ;
- Fondations et associations à buts sociaux, associations et fondations de soutien aux personnes ;
- Acteurs institutionnels en lien avec les addictions et dépendances ;
- Structures d'accueil de la petite enfance (crèches, garderies, etc.).

Outre l'appartenance au réseau, il est prévu que chaque service public partenaire du réseau désigne une personne répondante. Les personnes répondantes désignées, formées spécifiquement par l'UGM, seront les interlocutrices de premier recours lorsqu'une situation de menace se présente. Ces personnes pourront dans un premier temps réagir de manière appropriée aux situations[5] et dans un deuxième temps procéder à une première évaluation de la situation et estimer la gravité du cas. Si le cas est qualifié de risque aggravé de violence, la personne répondante annoncera le cas à l'UGM. Si le cas n'entre pas dans le champ d'application de la gestion des menaces, l'institution à laquelle appartient la personne répondante sera chargée de trouver des solutions adaptées au cas particulier, avec, si besoin, le soutien et les conseils de l'UGM.

[5] Il va de soi que le recours à la Police cantonale, via le 117, demeurera possible en tout temps.

Il convient de relever d'emblée que la fonction de personne répondante ne générera pas de travail supplémentaire au sein des services de l'Etat, si ce n'est une formation initiale et une formation continue chaque année, les deux sur une journée. Par ailleurs, cette désignation n'impliquera pas de valorisation de la fonction.

2.5.2 Mesures (ad art. 30j de l'avant-projet)

Les mesures proposées par le projet de loi restreignent les droits fondamentaux à différents degrés. Le projet présenté propose six types de mesures, qui peuvent être prises cumulativement, l'une n'excluant pas les autres. Dans tous les cas, il convient de rappeler que l'action de la Police cantonale est toujours guidée par le principe de proportionnalité et par le respect des droits fondamentaux (art. 30a al. 2 LPol).

Les mesures d'enquêtes (let. a) visent le travail de recoupement des informations et des éléments en possession de la Police cantonale et recueillis auprès des membres du réseau.

La collecte et le traitement des données (let. b) est absolument nécessaire pour le fonctionnement optimal du concept de gestion des menaces, dans le respect des principes de la protection des données, en particulier principes de finalité, de proportionnalité, d'exactitude et devoir de diligence accru (art. 5 à 8 LPrD). Il convient de relever qu'une confidentialité particulière devra être observée quant aux données en mains du service.

L'entretien préventif (let. c) a pour but de rencontrer la personne, d'évaluer son environnement social et personnel et de tenter de désamorcer la propension à la violence. Il a un but de désescalation de la situation, en particulier lorsqu'il s'agit de personnes en conflit avec un service de l'Etat ou en proie à des difficultés financières ou personnelles inextricables. L'expérience faite par d'autres cantons utilisant cet entretien préventif montre que dans la majorité des cas, non seulement les personnes à risques étaient tout à fait disposées à s'entretenir avec l'unité de gestion des menaces mais qu'en outre, cet entretien était l'occasion, pour les personnes à risques, de faire part de leurs problèmes et par là, se sentir écoutés et compris. Dans l'idéal, cet entretien volontaire devrait être tenu avant de recourir aux mesures évoquées ci-dessous.

Les mesures de soutien (let. d) visent à apporter des solutions durables pour les personnes à risques et leur entourage, comme la mise en place d'un suivi systémique de la personne à risques et de sa famille ou des mesures de suivi thérapeutique personnalisées. En effet, il est important de concevoir le concept de gestion des menaces non seulement comme une politique sécuritaire de gestion des risques mais aussi comme une politique à visée sociale.

Comme déjà mentionné plus haut (cf. chapitre 2.2), un concept de gestion des menace a également pour mission d'offrir un soutien aux partenaires institutionnels et privés dans la gestion de la menace et dans le suivi des personnes à risques. La lettre e) concrétise cette action de l'UGM.

Enfin, il est important qu'une mesure soit prévue pour permettre à l'UGM de requérir l'intervention policière en cas de danger sérieux (let. f). En effet, si la gestion des menaces est avant tout un concept visant à prévenir la menace, la réalisation de la menace et du risque peut devenir sérieuse. Dans ces cas, il convient de prévoir explicitement une telle compétence à l'UGM.

Par ces mesures, il s'agit de donner des outils légaux à l'UGM, laissant une certaine liberté d'appréciation dans la mesure à prendre en fonction de la personne à risque et de la typicité du cas individuel et en concertation avec le groupe d'expert-e-s.

2.5.3 Communication de données dans le cadre de la gestion des menaces (ad art. 38c, 38d et 38h de l'avant-projet)

Comme déjà expliqué plus haut (cf. chapitre 2.3.1), la collecte et la communication de données ainsi que le traitement de ces dernières à des fins de gestion des menaces constituent un point essentiel du concept de gestion des menaces, traité dans le chapitre de la LPol consacré au traitement des données de police.

Si la remontée d'informations du terrain auprès de l'UGM est réglée par les articles 30i (réseau d'annonce et partenariat) et 30j let. b (mesures) de l'avant-projet, il convient de prévoir les modalités selon lesquelles certaines informations peuvent être transmises aux victimes potentielles, aux partenaires, en dérogation aux règles générales de la LPrD, en particulier aux règles relatives à la collecte (art. 9), à la communication (art. 10-12) et à la destruction (art. 13). En effet, dès lors qu'un concept de gestion de menaces a pour objectif de réduire les risques et vise un intérêt public prépondérant qu'est la protection de la vie, il est primordial que certaines informations puissent être transmises directement et de manière simplifiée aux personnes concernées, afin d'écarter un danger sérieux les concernant. Cette communication simplifiée de données entre partenaires permet en outre d'identifier les risques concrets et d'éliminer les cas qualifiés de « bagatelle », relevant par exemple de mouvements d'humeur ou de malentendus. Il en va ainsi de l'efficacité des autorités, services et partenaires concernés par la gestion des menaces de pouvoir compter sur un bon flux d'informations.

Afin d'éviter des dérives dans la communication des données, le projet soumet cette communication à certaines conditions. Ainsi la communication doit se limiter au strict nécessaire (critère de la nécessité), doit être apte à atteindre le but visé (critère de l'aptitude) et doit être proportionnée au but visé (critère de la proportionnalité au sens étroit) ; le but visé étant entendu comme celui d'empêcher la survenance du danger. Ce danger doit en outre être sérieux, soit susceptible de porter gravement atteinte à l'intégrité physique, psychique ou sexuelle de tiers, au sens de l'article 30f de l'avant-projet. La communication d'informations entre partenaires concernés dans le cadre de la gestion des données ne consiste en aucun cas en une plateforme d'échange totalement ouverte et accessible à tous les partenaires impliqués. Il s'agit plutôt de concevoir comment les informations centralisées auprès de la Police cantonale peuvent être retransmises, dans des situations spécifiques et à des conditions précises, une fois le recoupement de toutes les informations effectué et dans le but de donner une information claire aux personnes, services et partenaires concernés.

Il convient également de régler les conditions dans lesquelles les agent-e-s de la Police cantonale et le personnel du Centre d'engagement et d'alarmes (CEA) peuvent, dans le cadre de leurs activités d'intervention, disposer des données des personnes à risque. L'accès à ces données par les policiers et policières et le personnel du CEA en intervention est conçu, au premier titre comme un moyen de protéger ces personnes de toute atteinte contre leur intégrité physique lors des interventions, mais aussi afin de mener l'intervention de police de la meilleure manière possible, par exemple en temporisant le contact avec la personne à risques, lorsque l'état psychique de la personne ne s'y prête pas actuellement, ou au contraire en donnant une priorité absolue à l'intervention, par exemple dans un contexte de violences domestiques.

Enfin, le projet règle la durée de conservation des données ainsi que les conditions selon lesquelles la personne à risques peut accéder aux données traitées à son sujet, en dérogation aux règles générales de la LPrD. Le but visé par la gestion des menaces implique en effet de prévoir des règles spécifiques. La personne à risques peut exercer son droit d'accès aux données traitées dans le cadre de la gestion des menaces. Toutefois la transmission des données concernant la personne à risques (et elle seule) peut être différée ou refusée si des intérêts privés ou publics s'y opposent. De tels intérêts

sont présents lorsque par exemple, l'intégrité physique, psychique ou sexuelle de tiers (ex. entourage, victime potentielle) est compromise par la transmission de ces informations. En effet, il serait particulièrement incohérent que par l'exercice du droit d'accès aux données garanti par la LPrD, la personne à risques puisse soit entraver l'action de protection de tiers, soit accéder à un moyen de contrecarrer l'action des autorités. Dans tous les cas, il s'agira de mettre en balance la garantie de droits fondamentaux, tant du point de vue des victimes potentielles de menaces sous l'angle du droit à la vie (et l'obligation de protection dont l'Etat est garant à cet égard) que des personnes dites à risques, sous l'angle de la protection de la sphère privée.

En ce qui concerne enfin la conservation des données collectées dans le cadre de la gestion des menaces, la durée est de 5 ans dès le dernier signalement. Cette durée de conservation se justifie afin de garantir une période de sûreté et ainsi, en cas de rechute durant cette période de sûreté, assurer un suivi basé sur l'historique complet de la personne. Cette durée garantit également un droit à l'oubli pour les personnes à risques.

2.5.4 Surveillance (ad art. 30k de l'avant-projet) et Haute surveillance (ad art. 30l de l'avant-projet)

Dès lors que les droits fondamentaux de la personne à risques sont affectés par la gestion des menaces et qu'un système simplifié de communication de données est mis en place, un système de contrôle complet est rigoureusement nécessaire. Le double système de contrôle proposé par le projet consiste en une surveillance continue (surveillance, art. 30k) exercée par le Directeur ou la Directrice de la sécurité et de la justice. Il est prévu qu'à intervalles réguliers, tous les deux mois par exemple, le Directeur ou la Directrice de la sécurité et de la justice soit informé-e des affaires en cours et de la marche de l'unité, en particulier sur le respect des règles et des processus en matière de protection des données et de tenue des fichiers. Quant à la surveillance périodique (haute surveillance, art. 30l), elle consistera en un rapport annuel que la Direction de la sécurité et de la justice transmettra au Conseil d'Etat, avec une statistique des cas qui se sont présentés durant l'année sous revue, un compte-rendu des processus en matière de traitement des données et une évaluation du traitement des affaires et des résultats obtenus. Le rapport devra répondre à des exigences de confidentialité particulièrement strictes, en particulier en s'assurant que les personnes ne soient pas reconnaissables. Ce rapport, une fois approuvé par le Conseil d'Etat, sera transmis pour information à l'Autorité cantonale de protection des données.

2.6 Evaluation du risque

L'évaluation du risque se fait sur la base des informations remontées du terrain. Cette évaluation, au même titre que la collecte et l'échange d'information et l'annonce des cas, est une partie centrale du travail effectué dans le cadre de la gestion des menaces. Il s'agit en effet d'effectuer un travail de tri, entre les personnes en proie à des mouvements d'humeur et les personnes à risques, à proprement parler.

Il incombera à l'UGM de procéder à une première évaluation, secondée ensuite par le groupe d'expert-e-s. Il sied de relever que des logiciels pour une première évaluation de la menace existent, tel que le logiciel Octagon utilisé par le canton de Zurich, dont la Police cantonale pourrait se munir après évaluation.

3 ADAPTATIONS AU SYSTÈME D'INFORMATION SCHENGEN (SIS II)

Pour rappel, la Suisse a conclu avec l'Union européenne un accord d'association à l'espace Schengen et est dès lors membre de l'espace Schengen depuis 2008. L'espace Schengen regroupe 26 Etats européens qui, par leur accord mutuel, ont décidé d'éliminer l'exigence du passeport et les contrôles d'immigration à leurs frontières nationales.

La mise en œuvre de l'accord d'association Schengen prévoit un système d'information informatisé (SIS II) qui vise à renforcer la sécurité et à faciliter la libre circulation au sein de l'espace Schengen. Le système a été institué en 2006 et a été mis en activité en avril 2013. Le SIS II facilite l'échange d'information entre les autorités nationales chargées des contrôles aux frontières, les autorités douanières et la police, concernant des personnes susceptibles d'avoir participé à des actes criminels graves. Il contient également des signalements se rapportant à des personnes portées disparues, notamment des enfants, ainsi que des informations sur certains biens, tels que les billets de banque, les voitures, les camionnettes, les armes à feu et les documents d'identité qui peuvent avoir été volés, détournés ou égarés.

L'article 36 de la décision 2007/533/JAI du Conseil de l'Union européenne du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) définit l'objectif des signalements concernant des personnes ou des objets aux fins de contrôle discret ou de contrôle spécifique, ainsi que les conditions auxquelles ces signalements sont soumis. Il est libellé de la manière suivante :

Article 36

Objectifs des signalements et conditions auxquelles ils sont soumis

1. Les données concernant des personnes ou des véhicules, des embarcations, des aéronefs ou des conteneurs sont introduites conformément au droit national de l'État membre signalant, aux fins de contrôle discret et de contrôle spécifique, conformément à l'article 37, paragraphe 4.

2. Un tel signalement peut être effectué pour la répression d'infractions pénales et pour la prévention de menaces pour la sécurité publique :

a) lorsqu'il existe des indices réels laissant supposer qu'une personne a l'intention de commettre ou commet une infraction pénale grave, telle qu'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI ; ou

b) lorsque l'appréciation globale portée sur une personne, en particulier sur la base des infractions pénales commises jusqu'alors, laisse supposer qu'elle commettra également à l'avenir des infractions pénales graves, telles que les infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/548/JAI.

3. En outre, le signalement peut être effectué conformément au droit national, à la demande des instances compétentes pour la sûreté de l'État, lorsque des indices concrets laissent supposer que les informations visées à l'article 37 paragraphe 1, sont nécessaires à la prévention d'une menace grave émanant de l'intéressé ou d'autres menaces graves pour la sûreté intérieure et extérieure de l'État. L'État membre procédant au signalement en vertu du présent paragraphe en tient informés les autres États membres. Chaque État membre détermine à quelles autorités cette information est transmise.

4. Des signalements relatifs aux véhicules, aux embarcations, aux aéronefs ou aux conteneurs peuvent être introduits lorsqu'il existe des indices réels de l'existence d'un lien entre ceux-ci et des infractions pénales graves visées au paragraphe 2 ou des menaces graves visées au paragraphe 3.

Afin de mettre en œuvre, au niveau national, les exigences du SIS II, le Conseil fédéral a arrêté l'Ordonnance du 8 mars 2013 sur la partie nationale du système d'information Schengen (N-SIS) et sur le bureau SIRENE[6] (Ordonnance N-SIS ; RS 362.0).

En vertu de l'art. 3 al. 1 de l'ordonnance N-SIS, l'office fédéral de la police (fedpol) est responsable de l'exploitation conforme au droit de ses systèmes d'informations, dont le N-SIS. Les cantons demeurent en revanche responsable pour la mise en œuvre des mesures (cf. art. 3 al. 3).

Une enquête du bureau SIRENE a été conduite afin de déterminer si les cantons disposaient d'une base légale applicable aux signalements selon l'art. 36 de la décision 2007/533/JAI du Conseil de l'Union européenne du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II). Il en est ressorti que Fribourg n'en disposait pas.

Afin de combler la lacune juridique cantonale découlant de la mise en œuvre du SIS II, il est proposé d'introduire, dans la loi du 15 novembre 1990 sur la Police cantonale un nouvel article.

4 RECHERCHE DE PERSONNES CONDAMNÉES

La nouvelle loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; RS 780.1) et ses ordonnances d'exécution sont entrées en vigueur le 1er mars 2018. Entre autres nouveautés, la LSCPT permet, à son article 36, la recherche de personnes condamnées dont la localisation est inconnue, possibilité jusqu'ici inexistante avec les bases légales actuelles. L'art. 37 LSCPT précise que : « *La Confédération et les cantons désignent l'autorité qui ordonne la surveillance, celle qui autorise la surveillance et l'autorité de recours. L'ordre de surveillance est soumis à l'autorisation d'une autorité judiciaire.* ».

L'article 36 LSCPT règle matériellement les conditions de la recherche de personnes condamnées ; il s'agit dès lors pour le canton de Fribourg de définir quelles sont les autorités habilitées à ordonner puis à autoriser de telles recherches, conformément à l'article 37 LSCPT.

La présente révision partielle de la LPol est l'occasion d'inscrire dans une disposition de droit formel le champ des compétences issu de l'article 36 LSCPT. A ces fins l'article 31c LPol a été reformulé pour comprendre désormais les compétences en matière de recherche de personnes condamnées. Il convient de préciser que le Conseil d'Etat a réglé, de manière provisoire le champ de compétences par voie d'ordonnance (ordonnance sur la surveillance de la correspondance par poste et télécommunication en cas de recherche de personnes condamnées ; RSF 551.41), afin de permettre aux autorités de mettre en œuvre l'article 36 LSCPT dès son entrée en vigueur.

4.1 Compétences actuelles en matière de localisation d'une personne disparue (art. 31c LPol)

Actuellement, dans le canton de Fribourg, l'article 31c LPol règle les compétences en matière de localisation des personnes disparues, en dehors de la procédure pénale et lorsque la santé et la vie de ces personnes sont gravement menacées. Une surveillance de la correspondance par télécommunication limitée à l'identification des usagers et aux données relatives au trafic peut alors être ordonnée pour retrouver une personne disparue (al. 1).

La Police cantonale est compétente, par un officier de police judiciaire, pour ordonner la surveillance de la correspondance par télécommunication pour retrouver une personne disparue (al. 3). L'ordre de surveillance est transmis dans les vingt-quatre heures, pour autorisation, au président de

[6] SIRENE : demande d'informations supplémentaires requises à l'entrée nationale (**S**upplementary **I**nformation **RE**quest at the **N**ational **E**ntry).

la Chambre pénale du Tribunal cantonal, qui examine si la mesure portant atteinte à la personnalité est justifiée (al. 4). Le président de la Chambre pénale statue dans les cinq jours à compter du moment où la surveillance a été ordonnée en indiquant brièvement les motifs. Il peut autoriser la surveillance à titre provisoire, demander que le dossier soit complété ou que d'autres éclaircissements soient apportés et exiger des mesures supplémentaires de protection de la personnalité (al. 5).

4.2 Compétences d'ordonner et d'autoriser la recherche de personnes condamnées (art. 36 LSCPT / 31c avant-projet LPol)

L'article 36 LSCPT prévoit la possibilité, nouvelle, d'avoir recours à une surveillance de la correspondance par poste et télécommunication pour rechercher une personne condamnée à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté, sur la base d'un jugement définitif et exécutoire.

La surveillance de la correspondance par poste et télécommunication visée à l'art. 36 LSCPT permet non seulement d'obtenir les données permettant d'identifier les usagers et les données relatives au trafic, c'est-à-dire des données secondaires, mais également le contenu des envois, dans le domaine de la correspondance par poste, et celui des communications, dans le domaine de la correspondance par télécommunication. Ceci se justifie, étant donné que le contenu des correspondances et des communications est susceptible de donner des renseignements sur le lieu où se trouve la personne condamnée et, dans le domaine de la correspondance par télécommunication, de permettre de vérifier si c'est vraiment elle qui utilise le raccordement surveillé.

Le nouvel article 31c LPol prévoit que la compétence d'ordonner la recherche appartienne à la Police cantonale (officier/ère de service) et la compétence d'autoriser la recherche au Tribunal des mesures de contrainte. Le recours contre les décisions du Tribunal des mesures de contrainte peut être formé auprès de la Chambre pénale du Tribunal cantonal, ce qui permet un double contrôle judiciaire de la mesure.

5 MODIFICATIONS MINEURES

5.1 Modification de la loi d'application de la législation fédérale sur la circulation routière (RSF 781.1)

En raison de la modification du 15 juin 2012 de loi fédérale sur la circulation routière (LCR, RS 741.01), entrée en vigueur le 1er janvier 2014, le renvoi de l'article 18 al. 1 LALCR n'est plus correct. L'infraction consistant à conduire un véhicule sans moteur alors que la personne se trouve dans l'incapacité de conduire doit être dévolue à la connaissance du Préfet. Il s'agit dès lors de corriger le renvoi à l'ancien article 91 al. 3 de la LCR qui a été remplacé par l'article 91 al. 1 let. c LCR.

5.2 Modification de la loi concernant la protection de l'enfant et de l'adulte (LPEA)

Selon la loi concernant la protection de l'enfant et de l'adulte (LPEA ; RSF 212.5.1), les juges de paix sont compétent-e-s pour ordonner des décisions de placement d'une personne à des fins d'assistance (art. 17 LPEA). Toutefois, pour faire exécuter leurs décisions de placement à des fins d'assistance, les juges de paix doivent requérir la Police cantonale par l'intermédiaire du préfet (art. 21 LPEA).

La présence d'un intermédiaire à la réquisition de la police ne se justifie plus, dès lors que les juges de paix ont, en tant qu'autorité judiciaire, la compétence directe de requérir l'intervention de la police, au sens de l'article 4 al. 2 let. c LPol.

En revanche, il est renoncé à permettre aux médecins de requérir directement la police. En effet, il est souhaitable que la réquisition soit opérée par une autorité judiciaire ou préfectorale. S'agissant des médecins, la réquisition de la police par l'intermédiaire du préfet est ainsi conservée.

5.3 Autres modifications

Un certain nombre de petites modifications sont opérées dans la LPol.

Le détail de ces modifications se trouve dans le commentaire des articles (cf. chapitre 6).

6 COMMENTAIRE DES ARTICLES

Art. 2 al. 1 let. f (nouvelle)

L'ajout de cette nouvelle lettre disposant que la Police cantonale a pour tâches de prévenir les infractions permet une assise légale à la mise en place du concept de gestion des menaces. Bien que le travail police, en soi, contribue déjà à prévenir un certain nombre d'infractions, il convient de régler explicitement cet aspect.

Art. 4 al. 1

Cette modification permet de préciser le champ missionnel de la Police cantonal dans le cadre des réquisitions par d'autres autorités. L'intervention de la Police cantonale doit ainsi se justifier par la nécessité du recours à la force publique. Il n'est plus conforme au principe de la proportionnalité et de l'efficience de la Police cantonale de faire intervenir des agent-e-s uniformé-e-s pour procéder à des notifications de commandements de payer ou des notifications judiciaires, par exemple.

Art. 7 al. 1, 11 al. 1, 14 al. 1, 20 al. 3 et 4, 25 al. 1, 26 al. 3, 33c al. 2

Pour tous ces articles, il s'agit de combler une lacune. En effet, actuellement, le remplacement du Commandant ou de la Commandante de la Police cantonale n'est pas explicitement réglé par la LPol.

Il est important, du point de vue opérationnel, qu'un-e remplaçant-e puisse suppléer une absence du Commandant ou de la Commandante. Il convient de relever qu'actuellement et dans les faits, un remplaçant du Commandant est désigné. Toutefois, ses attributions ne sont pas explicitement prévues par la LPol.

Le but de cette disposition n'est pas d'instaurer un co-commandement au sein de la Police cantonale mais bel et bien d'instaurer des règles en cas d'absence ou d'indisponibilité du Commandant ou de la Commandante de la Police cantonale.

Art. 10 al. 2

A ce jour, la majorité des postes décentralisés est déjà déterminée. A l'avenir, d'éventuels changements dans la localisation des postes décentralisés devraient être appréhendés sous l'angle opérationnel uniquement et non plus politique. Sous l'angle opérationnel, il est dès lors plus opportun de prévoir que ce soit la Police cantonale et le Directeur ou la Directrice de la sécurité et de la justice qui évaluent la pertinence de la localisation des postes de police décentralisés. Il convient finalement de souligner que la Police cantonale a un avantage certain à garder une répartition équilibrée de ses forces de police dans toutes les parties du canton, y compris dans régions périphériques ayant une densité de population moins importante.

Art. 11 al. 3 (nouveau), 14 al. 2 (nouveau)

Cette disposition a pour but de prévenir d'éventuelles situations de crises qui se présenteraient et nécessiteraient que les agent-e-s de la Police cantonale doivent porter leurs armes en dehors du service, afin d'augmenter le seuil de sécurité de la population. L'on pense par exemple aux menaces terroristes mais aussi pour les cas d'agent-e-s qui seraient directement menacé-e-s en raison de leur activité de policier (ex. agent-e-s agissant sous couverture dont l'identité réelle aurait été découverte).

Cette disposition n'entre pas en concurrence avec la loi fédérale sur les armes, les accessoires d'armes et les munitions (loi sur les armes, LArm ; RS 514.54) puisque la LArm exclut précisément les autorités policières de son champ d'application (cf. art. 2 al. 1 LArm).

Art. 13

La mention du stationnement, à Fribourg, de la Police de sûreté doit être supprimée. En effet, les besoins infrastructurels de la Police cantonale et plus particulièrement de la police de sûreté sont en évolution, de telle sorte qu'un déménagement de la police de sûreté dans l'agglomération fribourgeoise est prévisible. De même, il n'est pas exclu que des antennes de la police de sûreté soient créées dans le canton, afin de répondre aux développements de la criminalité.

Une limitation du stationnement à la ville de Fribourg n'est plus justifiée à ce jour.

Art. 15 al. 1 let. a)

La suppression de cette distinction entre gendarmerie et police de sûreté est nécessaire en raison de son obsolescence. En effet, avec le temps la Police cantonale a développé des services supports, à savoir le service des ressources humaines, les services généraux et les services du commandement. Il convient donc de laisser au Conseil d'Etat le soin de régler l'organisation des différents corps et services de la Police cantonale, d'une manière générale.

Art. 15 al. 1 let. b)

Au vu de la modification de la lettre a de cet article (cf. supra commentaire de l'article 15 al. 1 let a) qui prévoit que le Conseil d'Etat règle l'organisation de la Police cantonale de manière générale, il convient de supprimer cette lettre qui prévoit une distinction entre les différents corps et services de la Police cantonale.

Art. 18 al. 1

La nomination de tous les officiers et officières de la Police cantonale par le Conseil d'Etat est, en pratique, une procédure lourde qui n'est justifiée par aucun motif particulier. Par cette modification, le Conseil d'Etat nommera, à l'avenir uniquement les membres de l'Etat-major de la Police cantonale, soit le Commandant ou la Commandante, le/la remplaçant-e du Commandant ou de la Commandante, le/la chef-fe-e de la Police de sûreté, le/la chef-fe-e de la gendarmerie, le/la chef-fe-e des ressources humaines ainsi que le/la chef-fe-e des services généraux. Les autres nominations relèveront du Directeur de la sécurité et de la justice.

Art. 30f But

Cet article énonce le but de la gestion des menaces, soit la détection précoce et la prévention de la commission d'infractions, par des personnes (personnes à risques) dont le comportement ou les

propos laissent supposer une propension marquée à la violence dirigée contre des tiers et qui sont aptes à porter gravement atteinte à l'intégrité physique, psychique ou sexuelle de tiers.

Les cas d'application typiques de la gestion des menaces concernent notamment les violences domestiques, le harcèlement obsessionnel (stalking), les menaces substantielles, qu'elles soient ouvertes, cachées, anonymes ou identifiées, les comportements quérulents, les comportements violents liés à des troubles mentaux ou encore le harcèlement sexuel.

Les biens juridiques protégés sont prépondérants puisqu'il s'agit de l'intégrité physique, psychique ou sexuelle de tiers.

A relever enfin que cette disposition ne vise pas à prévenir les violences que la personne à risques pourrait diriger contre elle-même (suicide ou comportements auto-agressifs) pour autant que cette violence n'ait pas d'incidences sur des tiers.

Art. 30g **Organisation** a) Unité

Cette disposition institue une nouvelle unité de gestion des menaces au sein de la Police cantonale. Si, dans le cadre de la gestion des menaces, l'accent est mis sur la collaboration transversale et interdisciplinaire, il est toutefois nécessaire qu'une unité centralise et coordonne l'activité de gestion des menaces ; il apparaît particulièrement adéquat que cette unité soit intégrée au sein de la Police cantonale, dès lors que la recherche et le traitement d'information sur les personnes est un travail de police par excellence.

L'alinéa 2 résume l'activité de l'unité qui consiste à évaluer le risque au moyen des instruments d'analyse appropriés et de prendre les mesures idoines (au sens de l'article 30j LPol). C'est par cet alinéa également qu'est institué le réseau des partenaires institutionnels et privés qui sont désignés plus précisément à l'article 30i (réseau d'annonce).

L'alinéa 3 prévoit que l'unité soit placée sous la conduite du Commandant ou de la Commandante de la Police cantonale. En effet, vu la sensibilité du domaine, il paraît tout à fait justifié que la surveillance et la conduite appartienne au rang hiérarchique le plus élevé de la Police cantonale.

Enfin, par l'alinéa 4, il incombe au Conseil d'Etat de régler plus précisément l'organisation de l'unité par voie d'ordonnance.

Le détail de l'organisation est également décrit plus haut, au chapitre 2.5.1 (organisation).

Art. 30h b) Groupe d'expert-e-s

Cette disposition institue le groupe d'expert-e-s, organe consultatif opérant en appui du travail opérationnel de l'unité de gestion des menaces. Comme mentionné plus haut (cf. chapitre 2.5.1), un groupe d'expert-e-s est indispensable pour procéder à l'évaluation et au suivi des cas. Le groupe d'expert-e-s concrétise un des pans de la collaboration transversale et interdisciplinaire (l'autre pan étant constitué du réseau de partenaires institutionnels et privés et des personnes répondantes).

Le groupe d'expert-e-s est nommé par le Conseil d'Etat, sur proposition de la Direction de la sécurité et de la justice (al. 1). L'UGM sollicite le groupe d'expert-e-s lorsqu'une analyse spécialisée et un soutien à la décision sont nécessaires. Il s'agit là d'appuyer l'UGM dans les cas dont l'évaluation du risque est complexe.

Le détail de l'organisation est également décrit plus haut, au chapitre 2.5.1 (organisation).

Art. 30i Réseau d'annonce et partenariat

Cette disposition prévoit l'annonce des cas, par les partenaires institutionnels et privés du réseau ainsi que la collaboration entre ces derniers et l'UGM. L'annonce n'est pas obligatoire et la liste des partenaires privés appelés à annoncer les cas est exhaustive. Il sied de préciser que l'anonymat des personnes procédant à l'annonce est garantie, sous réserve des cas relevant de la dénonciation calomnieuse (art. 303 CP).

La lettre a institue la collaboration et l'annonce par les services publics de l'Etat et des communes ainsi que des corporations et établissements de droit public. Pour ces derniers, l'on pense par exemple à l'Etablissement de détention fribourgeois (EDFR) ou à l'hôpital fribourgeois (HFR). Les corporations de droit public particulièrement visées dans le cadre de la gestion des menaces sont les corporations ecclésiastiques reconnues, soit l'Eglise catholique romaine et l'Eglise évangélique réformée et la communauté israélite.

La lettre b institue la collaboration et l'annonce par les autorités du pouvoir judiciaire.

La lettre c institue la collaboration et l'annonce par les partenaires des secteurs privés, lorsque le champ de leur compétence se situe dans l'accomplissement de tâches de droit public. L'on pense par exemple aux institutions et fondations de soutien aux personnes, aux familles, aux enfants, aux jeunes en difficultés, aux toxicomanes et aux personnes en situation de dépendance dont l'activité est financée par l'Etat, en totalité ou en partie.

La lettre d se réfère aux professionnel-le-s de la santé soumis à la loi sur la santé (LSan ; RSF 821.0.1) et tels que décrits par l'article 1 de l'ordonnance concernant les fournisseurs de soins (RSF 821.0.12). Il convient de relever qu'en pratique certaines professions seront particulièrement concernées par la gestion des menaces (ex. professionnel-le-s en lien avec la santé mentale) alors que d'autres ne devraient en principe être que peu concernées (ex. podologue ou technicien-ne-e dentiste).

Enfin, la lettre e prévoit la collaboration et l'annonce par des partenaires privés que sont les associations poursuivant un but social, de prévention ou de soutien ainsi que les associations religieuses. Les premières associations visées sont, comme pour la lettre c, les associations de droit privé dispensant un soutien aux personnes, aux familles, aux enfants, aux jeunes en difficultés, aux toxicomanes et aux personnes en situation de dépendance. Les associations religieuses visées par cet alinéa sont les communautés religieuses formées en association de droit privé qui ne sont pas reconnues comme corporation de droit public (cf. art. 30i, let. a), comme par exemple les communautés musulmanes.

Les alinéas 2 à 4 règlent le principe de la levée du secret de fonction et du secret professionnel, pour les professionnel-le-s de la santé et pour les ecclésiastiques, dans leurs relations avec l'UGM. Ces dispositions sont nécessaires et fondamentales, afin d'épargner aux personnes concernées par le réseau d'annonce, des poursuites pénales au sens des articles 320 et 321 CP (violation du secret de fonction et violation du secret professionnel). S'agissant des ecclésiastiques, il convient de préciser que cette notion inclut les évêques, les prêtres et les pasteurs des communautés chrétiennes, mais aussi les prédicateurs des autres religions, tels que les rabbins, imams et chefs bouddhistes[7].

Art. 30j Mesures

Cet article dresse une liste de mesures que l'unité de gestion des menaces peut prendre lorsqu'une personne à risques est identifiée et qu'il y a lieu de craindre qu'elle commette une infraction. Ces

[7] Cf. DUPUIS Michel et al., *Petit commentaire du Code pénal (PC CP)*, p. 2023, Bâle, 2017.

mesures sont exhaustivement réglées par la loi ; elles peuvent être prises cumulativement, l'une mesure n'excluant pas une autre.

La lettre a institue le travail d'enquête de l'unité de gestion des menaces en vue d'évaluer la dangerosité de la personne. Il s'agit principalement de mesures de recherches et de recoupements d'informations sur la personne. En fonction de l'évaluation de la dangerosité, la personne à risques pourrait être annoncée et suivie par le service d'enquête compétent, en particulier les services de renseignement.

La lettre b règle la question de la collecte et du traitement des données par l'unité de gestion des menaces. L'unité de gestion des menaces est autorisée à traiter et recouper des données, y compris des données sensibles afin d'assurer la prévention et la détection précoce d'infractions ainsi que le suivi des personnes à risques.

La lettre c permet à l'unité de gestion des menaces de procéder à des entretiens préventifs avec la personne à risques. Ces entretiens s'inscrivent dans les schémas de désescalade des comportements violents et servent à désamorcer une situation de crise. Cet entretien préventif permet également de contextualiser le comportement de la personne à risques, au regard de son environnement personnel, social et/ou familial. L'entretien préventif est un mode d'intervention éprouvé afin d'identifier les facteurs de risque auprès de la personne et d'identifier les mesures de prévention appropriées.

La lettre d prévoit une mesure orientée sur la résolution des problèmes. En effet, les mesures de soutien à la personne à risques et à son entourage sont un aspect important du concept de gestion des menaces, dès lors que le concept vise, outre la prévention des infractions, à aider la personne à risques à sortir d'une situation difficile.

La lettre e permet à l'UGM d'offrir un soutien aux partenaires institutionnels et privés dans la gestion de la menace et dans le suivi des personnes à risques.

Enfin, la lettre f réserve la possibilité, pour l'unité de gestion des menaces de déclencher l'intervention policière en cas de danger sérieux.

Pour le détail des mesures, il est renvoyé au chapitre 2.5.2 (Mesures).

Art. 30k Surveillance

Cet article instaure la surveillance continue, qui incombe au Directeur ou à la Directrice de la sécurité et de la justice.

La Direction de la sécurité et de la justice détermine les modalités de cette surveillance, sous le contrôle du Conseil d'Etat (cf. article 30l).

Art. 30l Haute surveillance

Cet article institue le Conseil d'Etat comme autorité exerçant la haute surveillance sur les activités relatives à la gestion des menaces. Il est prévu que la Direction de la sécurité et de la justice transmette annuellement un rapport au Conseil d'Etat. Le rapport contiendra une statistique des cas, un compte-rendu des processus en matière de traitement des données et une évaluation du traitement des affaires et des résultats obtenus.

Une fois approuvé, le rapport sera transmis à l'Autorité cantonale de protection des données, pour information.

Art. 31b al. 1 let. b

La version française est libellée de la sorte : « *lorsque le comportement de la personne donne de sérieuses raisons de soupçonner qu'elle est sur le point de commettre un crime ou qu'elle en prépare un* ». La version allemande quant à elle diverge de la version française en tant qu'elle inclut la notion de « crime grave » (schweres Verbrechen).

Il s'agit de corriger cette divergence et de ne garder que la notion de crime, dans les deux langues.

Art. 31 c Recherche en cas d'urgence et recherche de personnes condamnées

Cette disposition est modifiée afin de régler les nouvelles compétences issues de la législation fédérale en matière de recherche de personnes condamnées, selon l'article 36 de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; RS 780.1), qui règle les modalités de la recherche des personnes condamnées.

Reformulée, cette disposition désigne les différentes compétences en matière de recherche de personnes condamnées et des personnes disparues. Il incombe à la Police cantonale d'ordonner la recherche des personnes condamnées, au Tribunal des mesures de contrainte de l'autoriser et à la Chambre pénale du Tribunal cantonal de connaître les recours des personnes dont la surveillance par poste ou par télécommunication a été autorisée.

Art. 33 al. 2, 33a al. 1, 33b al. 1, 33c al. 1

La notion d'officier ou d'officière de police judiciaire est remplacée par la notion d'officier ou d'officière de service. Cela permet de clarifier la mission des officiers et officières de police judiciaire qui sont habilités désormais à prendre les décisions que leur confère la loi dans le cadre missionnel défini par leur hiérarchie et dans le cadre du service demandé pour certaines missions.

Un officier ou une officière de service dispose de la qualité d'officier ou officière de police judiciaire. Il s'agit dans les deux cas de cadres de l'échelon 3 et 4 au sein de la Police cantonale, cadres qui ont suivi une formation particulière, leur donnant la compétence de décider certaines mesures de contrainte. Il s'agit notamment des mesures de contrainte prévues par l'article 148 al. 2 de la loi sur la justice.

Ainsi la notion d'officier ou d'officière de service inclut celle actuelle d'officier/officière de police judiciaire (affaires de permanence), et celle d'officier/officière en activité (affaires hors permanence, notamment dans le cadre d'engagements planifiés).

Art. 33d

Par cette disposition, une base légale est introduite pour permettre à la Police cantonale d'effectuer les signalements prévus le système SIS II dans le cadre de la mise en œuvre de l'accord d'association Schengen.

Art. 38c al. 1

Cette disposition est modifiée pour inclure la collecte de données sensibles dans le cadre de la gestion des menaces, et non plus seulement pour les besoins d'une enquête en cours.

Art. 38d al 1ter

Il s'agit d'introduire un nouvel alinéa qui règle la durée de conservation des données enregistrées dans le cadre de la gestion des menaces.

La durée prévue est de 5 ans dès le dernier signalement en lien avec la gestion des menaces. Cette durée est jugée opportune pour permettre de garantir une période de sûreté suffisante et le critère du signalement auprès de l'unité de gestion des menaces est le critère le plus objectif. Cette durée permet également de garantir le droit à l'oubli pour les personnes à risques.

Art. 38h Communication de données dans le cadre de la gestion des menaces

Cette nouvelle disposition permet d'instaurer une communication de données dans le cadre de la gestion des menaces.

Le premier alinéa règle la manière dont la Police cantonale peut transmettre des informations à d'autres services ou partenaires et à des tiers lorsque la prévention d'un danger sérieux impose cette communication et ce en dérogation aux règles de la LPrD. La communication ne consiste en aucun cas en une plate-forme d'échange entre partenaires concernés mais en une communication ciblée émanant de l'unité de gestion des menaces et dans des situations précises. La communication doit se limiter au strict nécessaire (critère de la nécessité), doit être apte à atteindre le but visé (critère de l'aptitude) et doit être proportionnée au but visé (critère de la proportionnalité au sens étroit) ; le but visé étant entendu comme celui d'empêcher la survenance du danger. Ce danger doit en outre être sérieux, soit porter gravement atteinte à l'intégrité physique, psychique ou sexuelle de tiers, au sens de l'article 30f de l'avant-projet.

L'alinéa 2 règle les modalités de l'accès des agent-e-s de la Police cantonale et du personnel de la Centrale d'engagement et d'alarmes (CEA) aux informations collectées dans le cadre de la gestion des menaces. Cet accès se justifie afin d'assurer la sécurité des agent-e-s en intervention mais aussi pour la sécurité de tiers. L'accès à ces informations par les agent-e-s et le personnel du CEA en intervention permet également de garantir le suivi circonstancié des cas. L'accès à ces informations doit faire l'objet d'un contrôle de connexions au système qui permettra la mise à disposition des informations sur les personnes à risques. Le système est prévu comme un système d'alerte et non comme une somme d'informations à libre disposition du personnel visé par cette disposition.

Enfin, l'alinéa 3 règle les modalités selon lesquelles la personne à risques peut accéder aux données personnelles qui sont traitées par l'unité de gestion de menaces. La règle proposée est que la personne à risques puisse accéder à ses données personnelles mais que cet accès peut lui être refusé ou être différé en présence d'intérêts publics ou privés prépondérants. De tels intérêts sont présents lorsque par exemple, l'intégrité physique, psychique ou sexuelle de tiers est compromise par la transmission de ces informations.

Art. 90a al. 2 let a^{bis} LSan

Cette disposition crée une base légale permettant aux professionnel-le-s d'être délié-e-s du secret professionnel pour annoncer les cas de personnes à risques à l'unité de gestion des menaces. La levée du secret professionnel est indispensable afin d'éviter des poursuites pénales ultérieures aux professionnel-le-s de la santé.

Cette annonce n'est pas obligatoire. A cet égard, dans le cadre de la gestion des menaces, l'accent est mis sur la responsabilité d'annoncer. Cette annonce, laissée à la libre appréciation des professionnel-le-s de la santé, est également conçue comme un allègement de la responsabilité, puisque par l'annonce, l'appréciation de la dangerosité passe ensuite à l'unité de gestion des menaces et au groupe d'expert-e-s. En ce sens, en cas de doute sérieux sur la dangerosité, il est toujours profitable d'en informer l'unité de gestion des menaces.

Art. 18 al. 1 LALCR

La modification de cet article est nécessaire afin de corriger un renvoi à la loi fédérale sur la circulation routière (LCR ; 741.01). En effet, la modification du 15 juin 2012 de la LCR, entrée en vigueur le 1er janvier 2014, demande de remplacer le renvoi à l'article 91 al. 3 par l'article 91 al. 1 let. c LCR (conduite d'un véhicule sans moteur alors que la personne se trouve dans l'incapacité de conduire dévolue à la connaissance du Préfet).

Art. 21 al. 1 et 1bis LPEA

Cette disposition est modifiée pour permettre aux juges de paix de réquisitionner directement la police, sans passer par l'intermédiaire du préfet. Cette réquisition directe est conforme à l'article 4 al. 2 let. c LPol, dès lors que les juges de paix sont des magistrat-e-s et sont donc considéré-e-s comme une autorité judiciaire.

L'alinéa 1 est ainsi modifié pour permettre la réquisition directe de la police par les juges de paix.

L'alinéa 1bis est ajouté pour prévoir la réquisition indirecte de la police (par l'intermédiaire du préfet) par les médecins.

7 CONSÉQUENCES DU PROJET

7.1 Conséquences financières et en personnel

Les conséquences financières sont essentiellement des dépenses ordinaires en mobilier de bureau nécessaire pour la création de l'unité de gestion des menaces, qui sera située dans l'un des bâtiments de la Police cantonale, à Granges-Paccot (Madeleine 1, 3 ou 8, selon les capacités disponibles au début 2020).

L'équipement informatique ordinaire de l'unité de gestion des menaces n'aura pas d'incidences financières extraordinaires et sera pris sur le budget ordinaire, dès 2020.

L'opportunité de l'achat du logiciel Octagon développé par le canton de Zurich devra encore être examinée par la Police cantonale lorsque l'Unité de gestion des menaces sera mise en place et opérationnelle. Le prix exact du logiciel n'est pas encore connu et le sera vraisemblablement au premier semestre 2019. Le cas échéant, il s'agira également de prendre en compte les coûts d'adaptation du logiciel Octagon avec les logiciels usuels de la Police cantonale (SAGA/Zephyr). En l'état actuel des connaissances, ces besoins informatiques spécifiques peuvent être évalués à un montant de l'ordre de 80 000 à 100 000 francs.

Ces montants seront portés au budget 2020 de la Police cantonale.

S'agissant des incidences en personnel, l'unité de gestion de menaces nécessitera un total de 2,5 EPT : 1 chef-fe de l'unité de gestion des menaces à 100 %, 1 attaché-e du/de la chef-fe de l'unité de gestion des menaces à 100 % et 1 psychologue/criminologue à 50 %. Ces 2,5 EPT seront pris sur le contingent ordinaire de la Police cantonale, moyennant des transformations de postes. Le coût total de ces incidences en personnel est estimé à environ 110'000 francs par année.

Il convient enfin de relever que la fonction de personne répondante au sein du réseau d'annonce ne générera pas de travail supplémentaire au sein des services de l'Etat, si ce n'est une formation initiale et une formation continue chaque année, les deux sur une journée. Par ailleurs, cette désignation n'impliquera pas de valorisation de la fonction.

7.2 Incidences sur la répartition des tâches Etat-communes et conformité au droit supérieur et évaluation de la durabilité du projet

Le projet n'aura pas de conséquences sur le plan de la répartition des tâches entre l'Etat et les communes. La seule incidence directe sur les communes concerne la participation des services communaux au réseau des partenaires institutionnels et privés. Il leur incombera de désigner une personne répondante auprès des services concernés et délimités par l'unité de gestion des menaces. En outre, la possibilité est donnée aux communes d'annoncer les cas de personnes à risques à l'unité de gestion des menaces.

Le présent projet est compatible avec le droit de rang supérieur, soit le droit européen, le droit fédéral ainsi que la Constitution cantonale.

L'examen de la durabilité effectué pour le projet de révision sur les critères pertinents de l'évaluation amène à un résultat très favorable du projet de révision.