Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Direction générale
de la police nationale

Direction générale
de la gendarmerie nationale

Direction des affaires criminelles
et des grâces

Direction générale des douanes
et des droits indirects

Direction générale de la concurrence,
de la consommation et de la répression des fraude

Paris, le

19 JUIL. 2013

Le directeur général de la police nationale
Le directeur général de la gendarmerie nationale
La directrice des affaires criminelles et des grâces
Le directeur général des douanes et des droits indirects
La directrice générale de la concurrence, de la consommation
et de la répression des fraudes

à

Monsieur le Préfet de police
Mesdames et messieurs les préfets de régions et de départements
de métropole et d'outre-mer

et, pour information, à

Mesdames et messieurs les premiers présidents de cour d'appel et
le président du tribunal supérieur d'appel
Mesdames et messieurs les procureurs généraux et le procureur de la République près ledit tribunal
supérieur d'appel
Mesdames et messieurs les présidents de tribunaux de grande instance
Mesdames et messieurs les procureurs de la République
Monsieur le directeur de l'école nationale de la magistrature
Madame la représentante nationale auprès d'Eurojust

NOR/INT/C/ 1318958C

Objet : **Dispositif national de signalement des contenus illicites de l'Internet**

Annexe : **Protocole de compétences et glossaire**

La présente circulaire a pour objet de présenter les modalités de fonctionnement de la Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements (PHAROS), dispositif interministériel de signalement des contenus illicites de l'Internet.

I - Présentation générale

P.H.A.R.O.S. est placée au sein de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication de la direction centrale de la police judiciaire.

Elle est dirigée en alternance, par un fonctionnaire de la police nationale ou par un militaire de la gendarmerie nationale. Elle est composée à parité de policiers et de gendarmes, et a vocation à intégrer des fonctionnaires des autres administrations concernées par le dispositif.

Pour l'exercice de ses missions, P.H.A.R.O.S. met en œuvre un traitement de données à caractère personnel, créé par l'arrêté du 16 juin 2009 publié au Journal officiel du 20 juin 2009, et reposant sur l'exploitation du site Internet www.internet-signalement.gouv.fr, lancé le 6 janvier 2009, qui ouvre le dispositif au grand public et canalise un flux important d'informations.

Les missions de la plate-forme sont les suivantes :

• **prévention et renforcement des droits des internautes**- Le site www.internet-signalement.gouv.fr constitue un point de repère pour le public lorsqu'il se trouve confronté à des contenus illicites de l'Internet (information sur ses droits et démarches légales possibles ; espace documentaire, présentant des conseils de prévention, le dispositif de signalement et la législation relative à l'Internet) ;

• **accélération du traitement des signalements** - L'existence d'un pôle central, clairement identifié et joignable sans intermédiaire, optimise la transmission des informations, dans des délais de traitement compatibles avec la courte durée de vie des éléments d'enquête sur internet ;

• **rationalisation du traitement des signalements** - La délinquance « en ligne » est caractérisée par l'absence de critère territorial établi au moment du constat des infractions. Souvent, pour un même contenu, une multiplicité de signalements conduit différents services à diligenter parallèlement des enquêtes sur les mêmes faits. www.internet-signalement.gouv.fr, canal de convergence de l'information, recoupe les nouveaux signalements avec ceux déjà reçus, avant de les orienter, si nécessaire, vers les services compétents ;

• **mise en œuvre d'un outil de synthèses exploitable en termes de politiques publiques nationales et internationales** - L'existence d'un dispositif centralisé permet d'avoir une vision globale de la criminalité sur Internet et d'en cerner les nouvelles tendances. Cette action ne doit pas être confondue avec une veille proactive de la « toile », développée par d'autres services dans leurs domaines de spécialité respectifs.

II - Alimentation et consultation de la plate-forme nationale de signalement

La plus-value du dispositif repose sur sa capacité à fédérer, dans une démarche exhaustive, les sources de signalements de contenus illicites de l'Internet. Il s'agit principalement des internautes, des fournisseurs d'accès et de services sur Internet, des services de veille et services d'enquête étatiques. Tous ces acteurs peuvent utiliser le site www.internet-

signalement.gouv.fr pour communiquer directement des informations à la plate-forme, en temps réel.

Ainsi les services et unités d'enquête, notamment les services et unités territoriaux, régulièrement sollicités par le public pour recevoir les signalements de contenus illicites publiés sur Internet, doivent privilégier l'utilisation de cet outil plutôt que diligenter des procédures qui aboutissent à leur dessaisissement, faute de compétence territoriale.

Les services et unités d'enquête tout particulièrement actifs sur Internet - notamment les services de veille - doivent prendre en compte le fait que les contenus ou comportements qu'ils détectent au cours de leurs recherches peuvent fortuitement recouper des signalements reçus par P.H.A.R.O.S. La plate-forme constitue pour ces services et unités un outil de coordination incontournable :

• leur accès à la base de données leur permet de s'assurer de l'absence d'enquête en cours connue de P.H.A.R.O.S. concernant un contenu illicite. Les enquêteurs peuvent effectuer des recherches à partir de liens U.R.L., adresses e-mail, pseudonymes notamment. Cette faculté sera bientôt étendue à tous les services et unités territoriaux de police et de gendarmerie, ainsi qu'aux douanes et à la direction générale de la concurrence, de la consommation et de la répression des fraudes ;

• réciproquement, ils doivent signaler à la plate-forme les contenus ou comportements illicites relevés au cours de leurs investigations. Un formulaire de signalement simplifié sur www.internet-signalement.gouv.fr est mis à leur disposition pour faciliter ces transmissions.

III - Compétence de la plate-forme nationale de signalement

P.H.A.R.O.S. n'a pas vocation à recueillir des plaintes, mission distincte qui reste de la compétence des procureurs de la République et des services et unités d'enquête. Elle recueille des signalements, qui ont valeur de renseignements et peuvent justifier l'ouverture d'enquêtes.

La plate-forme est compétente pour recevoir le signalement de *contenus publics ou susceptibles d'être signalés parallèlement par plusieurs personnes*. Ce critère est lié aux modes de diffusion des contenus : sites Internet, forums, blogs, réseaux sociaux, échanges de fichiers de pair à pair (*peer to peer*), discussions fortuites sur des réseaux de discussion (*M.S.N.*, *tchat*, etc.) Tout type d'infraction peut être concerné : pornographie enfantine, incitation à la haine raciale, diffusion de procédés permettant la fabrication d'engins explosifs, escroquerie, contrefaçon, etc.

En conséquence, P.H.A.R.O.S. n'a pas vocation à recevoir :

• le signalement d'infractions matérialisées ou révélées par des correspondances entre personnes mutuellement identifiées (par exemple, des e-mails de menaces) ;

• le signalement d'infractions pour lesquelles seul un dépôt de plainte de la victime autorise le déclenchement de poursuites (injure, diffamation, etc.) ;

• le signalement de faits relevant de l'urgence opérationnelle : la plate-forme nationale de signalement n'est pas l'équivalent sur Internet d'un appel d'urgence au « 17 »

Le site de signalement précise aux internautes les démarches à entreprendre dans ces situations (dépôt de plainte, appel au « 17 », ...)

IV - Modalités de l'orientation des signalements et de leur prise en compte

4.1 - Détermination des destinataires

Chaque signalement est transmis à un unique destinataire *pour attribution*. Ce service ou unité est chargé d'y donner les suites qui s'imposent, opérationnelles, administratives et judiciaires. Il peut le traiter lui-même ou le transmettre pour attribution à un service ou unité d'enquête placé sous son autorité. Parallèlement, la nature d'un signalement peut imposer de le transmettre à un ou plusieurs destinataires *pour information*.

Un *protocole de compétences,* annexé à la présente circulaire, établit la répartition des signalements en fonction de critères matériels (infractions et modes opératoires) et territoriaux. Il énumère sur une *table de concordances* les critères retenus et les services et unités respectivement compétents pour traiter chaque type de signalement.

Dans les cas les plus spécialisés (terrorisme, trafic de cigarettes, trafic d'armes, groupements de pirates informatiques…), ce protocole ne retient pas un critère de compétence territoriale, le destinataire de la transmission étant un service ou unité à compétence nationale.

Dans les autres cas, le critère de la compétence territoriale s'applique : le destinataire d'une transmission est alors un service ou une unité territoriale. Le protocole de compétences prévoit deux types de *ventilation territoriale* :

• la ventilation territoriale de niveau 1 (V.T.N. 1), associée à des contenus ressortissant à la petite et à la moyenne délinquance (provocation directe au suicide, incitation à l'émeute…) ;

• la ventilation territoriale de niveau 2 (V.T.N. 2) associée à des contenus ressortissant à la criminalité organisée ou particulièrement sensibles (proxénétisme, apologie de crime de guerre et contre l'humanité, exercice illégal de la médecine…).

Dans le cadre d'une ventilation territoriale, la plate-forme recherche une localisation pertinente, de telle sorte que le destinataire pour attribution puisse effectuer un maximum d'investigations sur son propre ressort territorial. Il s'agit prioritairement du *lieu où le contenu signalé a été conçu.*

Par exception, si ce lieu ne peut être déterminé sans des investigations de terrain ou d'une particulière complexité, le critère retenu est la localisation d'un fournisseur d'accès local (réseau universitaire, réseau de grandes entreprises...) ou du serveur hébergeant les données illicites lorsqu'il est situé sur le territoire national. De même, un signalement dont l'exploitation judiciaire implique l'audition préalable d'une victime ou d'un témoin, peut être orienté vers le service ou unité compétent au titre du domicile de celui-ci.

Lorsqu'une ventilation territoriale est prévue, mais qu'aucun élément territorial ne ressort des investigations de la plate-forme, l'office central prévu, le cas échéant, comme destinataire pour information, peut devenir destinataire pour attribution.

Le protocole de compétences doit être appliqué avec discernement, sans qu'une lecture trop rigide ne conduise à des transmissions inopportunes. Lorsque les particularités d'un signalement imposent de déroger à la table de concordances ou lorsque le contenu signalé est d'une particulière gravité ou susceptible d'une résonance médiatique, un avis doit être sollicité par la plate-forme auprès du parquet territorialement compétent.

Lorsqu'une ventilation territoriale s'applique à un département autre que Paris et les trois départements limitrophes, le signalement est envoyé pour information au service ou à l'unité homologue de gendarmerie ou de police qui n'a pas été rendu destinataire pour attribution du fait notamment de la localisation du critère territorial en dehors de sa zone de compétence (exemple : si un groupement de gendarmerie est rendu destinataire d'un signalement pour attribution, la DIPJ correspondant est servie pour information).

Le service technique de recherches judiciaires et de documentation (S.T.R.J.D.) de la gendarmerie nationale est servi pour information dans tous les cas où une unité de la gendarmerie nationale est servie pour attribution. La D.C.S.P. est servie pour information dans tous les cas où un service de sécurité publique est servi pour attribution.

4.2 - Transmission et réception des signalements

Les signalements sont transmis à des messageries fonctionnelles. Pour garantir leur exploitation rapide, ils ne sont pas adressés à des messageries personnelles, sauf exception motivée.

Si les éléments déjà recueillis le justifient, la plate-forme nationale de signalement appelle l'attention des destinataires, dans sa transmission, sur la nécessité de veiller, en application des articles 65 et 65-3 de la loi du 29 juillet 1881, à l'éventuelle courte prescription - trois mois ou un an - des faits signalés, et de prendre l'avis du parquet territorialement compétent en cas de difficultés.

La transmission des signalements permet aux différents destinataires d'un signalement - pour attribution comme pour information - de s'identifier mutuellement, de telle sorte qu'ils puissent se contacter pour coordonner leur action.

Un accusé de réception est sollicité auprès des destinataires pour attribution.

Bien que la transmission la plus directe possible des signalements aux services et unités chargés de les exploiter soit souhaitable, certains relais ont été retenus, pour des nécessités de coordination. Il leur revient de répercuter les signalements vers les services et unités d'enquêtes placés sous leur autorité et de s'assurer de leur prise en compte effective.

La présente circulaire fixe les principes de détermination de la compétence des services et unités désignés dans le protocole, visant à accélérer la prise en compte des signalements.

Les destinataires pour attribution ont la possibilité, ponctuellement, de se déclarer incompétents. Ces déclarations doivent être exceptionnelles et expressément motivées. Il convient alors de prendre attache dans de brefs délais avec le parquet territorialement compétent et avec la plate-forme PHAROS, en proposant un nouveau destinataire. C'est à la plate-forme qu'il revient de faire la nouvelle transmission. En cas de désaccord persistant, la plate-forme nationale de signalement doit en aviser le parquet territorialement compétent, pour recevoir ses instructions.

Conformément aux textes qui ont fixé les attributions des offices centraux, ces derniers, lorsqu'ils sont rendus destinataires pour information de signalements, peuvent exercer leur faculté d'évocation et pour cela, prendre directement attache avec les services et unités territoriaux rendus destinataires pour attribution.

Les signalements qui parviennent à la plate-forme, relatifs à un même contenu déjà traité, ne sont pas automatiquement répercutés vers le service ou l'unité destinataire du premier signalement. Ils peuvent être sollicités auprès de la plate-forme pour répondre à des besoins tels que la mesure de l'impact médiatique d'un contenu illicite, l'identification de nouvelles victimes, etc.

4.3 - Traitement des signalements par leurs destinataires

Les signalements, dont les références sont adressées par messagerie à leurs destinataires, sont consultables à partir de l'application PHAROS, via les systèmes CHEOPS et PROXIMA. L'application inclut un espace intitulé « *Documentation professionnelle* », qui présente les modalités de son utilisation par les services et unités d'enquête, la méthodologie de traitement des signalements, les coordonnées d'hébergeurs de sites Internet et des aides à l'investigation dans le domaine de la cybercriminalité.

La mention de destinataires pour information ne dispense pas le destinataire pour attribution des avis habituellement donnés par les services et unités d'enquête lors de la constatation de faits particulièrement graves ou sensibles : l'information de l'autorité judiciaire et celle de l'autorité administrative.

La transmission d'un signalement par la plate-forme nationale de signalement n'est en aucune manière synonyme de déclenchement des poursuites, sauf si elle s'accompagne de la transmission d'une procédure (voir 4.4 - A). Le service ou l'unité destinataire pour attribution a la maîtrise de l'information qui lui est transmise et des modalités de son exploitation. Il lui incombe de contacter son parquet de rattachement pour l'informer des faits, conformément au code de procédure pénale et aux protocoles locaux.

Le service ou l'unité destinataire pour attribution est tenu de communiquer à la plate-forme nationale de signalement les suites judiciaires connues : C.O.P.J. (convocation par un officier de police judiciaire), ouverture d'information judiciaire, classement sans suite, etc. Il est mis à la disposition des services et unités d'enquête, sur l'application intranet « P.H.A.R.O.S. », une interface simplifiée permettant de cocher, rapidement et sans formalisme, les suites données.

Les enquêtes afférentes aux signalements étant susceptibles d'avoir une dimension technique, les enquêteurs peuvent, si nécessaire, obtenir un soutien opérationnel auprès de leurs référents spécialisés dans la lutte contre la cybercriminalité : investigateurs en cybercriminalité (I.C.C.) de la police nationale, gendarmes spécialisés en technologies numériques (N-TECH), référents « cybercriminalité » des directions départementales de la sécurité publique, gendarmes correspondants « technologies numériques » (C-NTECH) des groupements de gendarmerie départementale, cyberdouane etc.

Des copies d'écrans sont effectuées par la plate-forme nationale de signalement pour les contenus signalés qui le permettent. Elles visent à caractériser les éléments constitutifs des infractions relevées. Mesures conservatoires, elles sont transmises avec les signalements, sous forme de fichiers informatiques, et le cas échéant, sous forme d'annexes aux procédures de la plate-forme nationale de signalement. En dehors de cette dernière hypothèse, il revient au service enquêteur de les annexer à sa procédure ; il leur est alors reconnu valeur de constatations.

Dans tous les cas, cela dispense les destinataires des signalements de consulter en ligne les contenus signalés et leur évite les difficultés techniques (filtres des réseaux informatiques administratifs) et sécuritaires (risques d'infections virales) que ces consultations auraient supposées. Cependant, les nécessités d'une enquête et l'administration de la preuve, appréciées par les parquets locaux, peuvent impliquer de nouvelles consultations des contenus. Dans cette perspective, la plate-forme P.H.A.R.O.S. vérifie systématiquement l'innocuité des contenus signalés et alerte les destinataires de ses transmissions en cas de risque informatique. Si nécessaire, les services et unités destinataires des signalements sollicitent le soutien technique de leurs référents spécialisés dans la lutte contre la cybercriminalité (voir supra) qui disposent, le plus souvent, de connexions à Internet distinctes des réseaux administratifs, permettant d'effectuer des consultations sans risque.

Le destinataire du signalement pour attribution prend attache, si nécessaire, avec l'hébergeur du contenu signalé, pour « l'inviter à se conformer à son obligation de supprimer ce dernier » conformément aux articles 6–I-2 et 6–I-3 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Il peut s'agir au contraire de lui proposer d'observer un délai avant suppression, pour ne pas attirer l'attention de l'auteur du contenu avant qu'il ne soit entendu.

4.4 - Relations de la plate-forme P.H.A.R.O.S. avec les parquets

La plate-forme oriente les procédures entre les différents services enquêteurs selon le protocole de compétence annexé ; elle est, dès lors, peu amenée à entrer en contact avec les parquets. Néanmoins, elle devra prendre attache avec le parquet de Nanterre dans les hypothèses suivantes :

A - Lorsque la détermination du critère de compétence territoriale n'est pas possible sans des investigations plus poussées, les enquêteurs de la plate-forme PHAROS diligentent une enquête sous l'autorité du parquet de Nanterre. Ils doivent en outre nécessairement aviser ce parquet lorsqu'ils envisagent de demander une réquisition judiciaire. En cas de demande de réquisitions multiples pour un même signalement, rien ne s'oppose à ce que le parquet autorise, dans le cadre d'un document unique, plusieurs réquisitions, si celles-ci sont liées les unes aux autres. A l'issue de leurs investigations, dès lors qu'un critère de compétence territoriale est identifié, la procédure et un message d'information sont transmis au service enquêteur compétent.

B - Dans les cas prévus dans le protocole de compétences, il ne sera pas utile de contacter le parquet de Nanterre et la plate-forme pourra d'office transmettre les signalements aux services et unités territorialement compétents. Il appartiendra ensuite au service ou unité enquêteur à qui le signalement aura été transmis, d'aviser **immédiatement** le parquet de son ressort **pour confirmation ou infirmation de la saisine aux fins d'enquête**.

En revanche, pour des cas complexes, non prévus dans le protocole – pluralité des ressorts potentiellement compétents notamment - il sera nécessaire de contacter le parquet de Nanterre, seul compétent pour décider à quel parquet le signalement devra être transmis. Dans cette hypothèse, la plate-forme ne devra aucunement solliciter directement l'avis du parquet territorialement compétent.

C - En cas de doute sur l'orientation d'un signalement, ou dans le cas exceptionnel d'un litige relatif à la désignation d'un service ou unité d'enquête par la plate-forme de signalement (voir 4.2), cette dernière devra prendre attache avec le parquet territorialement compétent ou, faute de pouvoir le déterminer, le parquet de Nanterre qui décidera en dernier ressort.

V - Suivi du dispositif

Nous vous prions de bien vouloir porter à la connaissance de vos services les instructions portées dans la présente circulaire.

Le protocole de compétences annexé au présent sera révisé à des échéances qu'il conviendra de fixer. Vous inviterez les services et unités placés sous votre autorité à vous faire remonter toutes difficultés d'application du dispositif.

Le directeur général de la police nationale

Le directeur général de la gendarmerie nationale

La directrice des affaires criminelles et des grâces

La directrice générale des douanes et des droits indirects

La directrice générale de la concurrence, de la consommation et de la répression des fraudes

Nathalie HOMOBONO

Annexe à la circulaire interministérielle relative au dispositif national de signalement des contenus illicites de l'Internet
Protocole de compétences

Tableau de ventilation territoriale		
Localisation	**VTN1**	**VTN2**
Paris et petite couronne (92/93/94)	**DRPJ Paris** pour attribution du dossier à une DPJ ou à la DSPAP	**DRPJ Paris** pour attribution du dossier à une brigade centrale ou spécialisée ou à une DPJ
Autre département zone gendarmerie nationale	**Groupement de Gendarmerie** pour attribution du dossier à une brigade de recherche, une BDRIJ ou une brigade territoriale	**Région de gendarmerie** pour attribution du dossier à une section de recherche
Autre département zone police nationale	**DDSP** pour attribution du dossier à une circonscription de sécurité publique ou une sûreté départementale	**DIPJ**

Table de concordances

Catégorie matérielle	Réf	Domaine matériel	Source juridique	Destinataire pour attribution	Destinataires pour information
Racisme, antisémitisme et discriminations	1.1	Contestation de crimes contre l'humanité	Art. 24 bis de la loi du 29 juillet 1881	VTN2	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.2	Provocation publique à la haine et la discrimination raciale, ethnique ou religieuse*	Art. 24 al. 8 de la loi du 29 juillet 1881	VTN1 ou VTN2 selon gravité	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.3	Provocation publique à la haine et la discrimination à raison d'orientations sexuelles	Art. 24 al. 9 de la loi du 29 juillet 1881	VTN1 ou VTN2 selon gravité	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.4	Provocation publique à la haine et la discrimination à raison d'un handicap	Art. 24 al. 9 de la loi du 29 juillet 1881	VTN1 ou VTN2 selon gravité	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.5	« Happy slapping » à caractère xénophobe *	Art 222-33-3 CP	VTN1	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.6	Apologie de crime de guerre et contre l'humanité	Art. 24 al. 5 de la loi du 29 juillet 1881	VTN2	DCRI SDIG (DCSP) BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	1.7	Injures et diffamations xénophobes ou discriminatoires	Article 32 de la loi du 29 juillet 1881	Néant sauf cas particulier	Néant sauf cas particulier
Atteintes aux mineurs	2.1	Diffusion d'image ou vidéo pédopornographique (sauf Peer to Peer : voir 2.9)	Art. 227-23 al.1 CP	VTN1 ou VTN2 selon gravité	OCRVP / STRJD

	2.2	Corruption de mineur (« grooming ») Propositions de nature sexuelle à des mineurs	Art. 227-22 CP Art. 227-22-1 CP	VTN1 ou VTN2 selon gravité	OCRVP / STRJD
	2.4	Diffusion d'images à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine susceptible d'être vue par un mineur	Art. 227-24 CP	VTN1	OCRVP et STRJD en cas de contenu se rapportant à une affaire criminelle
	2.5	Réseaux d'adoption illégale	Art. 227-12 CP	OCRTEH	/
	2.6	Provocation des mineurs à l'usage ou au trafic de stupéfiants	Art. 227-18 et 227-18-1 CP	VTN1	OCRTIS
	2.7	Provocation des mineurs à la consommation d'alcool	Art. 227-19 CP	VTN1	OCLAESP
	2.8	Provocation des mineurs à la commission d'autres délits	Art. 227-21 CP	VTN1	Variable selon contenu
	2.9	Diffusion d'image pédopornographique par *peer to peer*	Art. 227-23 al.1 CP	Néant	STRJD (DLCC)
	2.10	Agression sexuelle sur mineur (dénonciation ou commission devant webcam)	Art. 222-22 CP	VTN1 ou VTN2 selon gravité	OCRVP / STRJD
Mouvements extrémistes	3.1	Provocation à s'armer contre la puissance publique ou une partie de la population	Art. 412-8 CP	VTN2	DCRI SDIG (DCSP) UCLAT BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	3.2	Provocations directes à commettre des crimes et délits diverses	Art. 24 de la loi du 29 juillet 1881	VTN1 ou VTN2 selon gravité	Variable selon contenu BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	3.3	Port ou exhibition d'uniformes, insignes ou emblèmes rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité	Art. R. 645-1 CP	VTN2	DCRI SDIG (DCSP) STRJD s'il s'agit de tenues militaires BLAT (DGGN) en cas de saisine d'une unité de gendarmerie
	3.4	Groupes de combat	Art. 431-13 et suivants CP	VTN2	DCRI SDIG (DCSP) STRJD BLAT (DGGN) en cas de saisine d'une unité de gendarmerie

Violences urbaines	4.1	Provocation à la rébellion	Art. 412-8, 431-6 et 433-10 CP	VTN1	CROGEND s'il s'agit d'une zone Gendarmerie
	4.2	Diffusion de procédés permettant la fabrication d'engins explosifs (contexte de VU)	Art. 322-6-1 CP	VTN2	SCAEMS IRCGN Institut National de Police Scientifique Bureau DUTOP (DCSP)
	4.3	Provocation directe à un attroupement armé	Art.431-6 CP	VTN1	CROGEND s'il s'agit d'une zone Gendarmerie
Terrorisme	5.1	Groupements et ententes terroristes	Art. 421-2-1 et 421-2-2 CP	UCLAT	
	5.2	Diffusion de procédés permettant la fabrication d'engins explosifs (contexte terroriste)	Art. 322-6-1 CP	UCLAT	IRCGN Institut National de Police Scientifique Bureau DUTOP (DCSP)
	5.3	Provocation aux actes de terrorisme et apologie	Art. 24 al. 6 de la loi du 29 juillet 1881	UCLAT	
	5.4	Menaces et actes d'intimidation dans un but terroriste	Art. 222-17 CP Art. R623-1 CP Art. 322-12 et 322-13 CP Art. R634-1 CP Art. 433-3 CP	UCLAT	
Trafics illicites	6.1	Trafic d'armes	Décret-loi du 18 avril 1939	OCLCO ou VTN2 selon gravité	UCLAT OCLCO SCAEMS BLAT (DGGN) s'il s'agit d'armes de guerre CYBERDOUANE EM DRPJ Paris
	6.2	Trafic de cigarettes authentiques ou de contrefaçon	Art. 414 et suivants du Code des Douanes	CYBERDOUANE	OCLCO
	6.3	Médicaments (trafics et contrefaçons)	Variable	OCLAESP	CYBERDOUANE
	6.4	Trafic de produits dopants	Articles 222-34 et suivants du CP	VTN2	OCLAESP CYBERDOUANE OCRTIS
	6.5	Recels divers	Art. 321-1 CP	VTN1 ou VTN2 selon gravité	Variable selon contenu

	6.6	Trafic d'animaux	Variable	VTN2 ou CYBERDOUANE s'il s'agit d'animaux visés par la convention de Washington	DGCCRF OCLAESP CYBERDOUANE si attribution VTN2
	6.7	Fausse monnaie	Art. 442-1 et suivants CP	VTN2	OCRFM
	6.8	Trafics de biens culturels	Variable	OCBC	CYBERDOUANE STRJD EM DRPJ Paris
	6.9	Atteintes au droit d'auteur	Code de la Propriété Intellectuelle	VTN1 ou VTN2 selon gravité	OCLCTIC
	6.10	Autres contrefaçons (de marques, etc.)	Variable	Néant *	CYBERDOUANE DGCCRF
	6.11	Trafic de stupéfiants (local)	Art. 222-34 et suivants CP	VTN1 ou VTN2 selon gravité	OCRTIS
	6.12	Trafic de stupéfiants national ou international	Art. 222-34 et suivants CP	OCRTIS	CYBERDOUANE EM DRPJ Paris
	6. 13	Trafic d'alcools	Code des Douanes	CYBERDOUANE	OCLCO
	6.14	Présentation des stupéfiants sous un jour favorable	Art L3421-4 CSP	VTN1	OCRTIS
Atteintes aux systèmes automatisés de traitement des données	7.1	Mise à disposition de programmes ou d'instruments conçus ou adaptés pour commettre des atteintes aux STAD	Art. 323-3-1 et 323-5 à 323-7 CP	VNT2 ou OCLCTIC selon gravité	DCRI STRJD (DLCC) OCLCTIC si attribution VTN2
	7.2	Infractions en matière de cryptologie	LCEN	VNT2 ou OCLCTIC selon gravité	DCRI STRJD (DLCC) OCLCTIC si attribution VTN2
	7.3	Groupement de pirates	Art. 323-4 CP	VNT2 ou OCLCTIC selon gravité	DCRI STRJD (DLCC) OCLCTIC si attribution VTN2
	7.4	Commande, conception, ou diffusion d'une publicité faisant la promotion d'un dispositif ou instrument conçu pour capter frauduleusement des programmes télédiffusés, lorsque ces programmes sont réservés à un public déterminé qui y accède moyennant une rémunération	Art 79-1 et 79-2 de la loi n°86-1067 du 30 septembre 1986 relative à la liberté de communication	OCLCTIC	/
Menaces	8.1	Menaces de violences contre des particuliers	Art. 222-17 CP Art. R623-1 CP	VTN1 ou VTN2 selon gravité	/
	8.2	Menaces de destructions	Art. 322-12 et 322-13 CP Art. R634-1 CP	VTN1 ou VTN2 selon gravité	/
	8.3	Actes d'intimidation envers les personnes exerçant une fonction publique	Art. 433-3 CP	VTN1 ou VTN2 selon gravité	/
Atteintes à la vie privée	9.1	Collecte illicite de données Traitement malgré opposition	Art. 226-18 et 226-18-1 CP 226-21 et 226-22	VTN2	OCLCTIC

	9.2	Fabrication et distribution de matériels permettant des atteintes à la vie privées	Art. 226-3 CP	VTN2 ou DCRI selon la nature des intérêts visés	Secrétariat général pour la Défense Nationale (Matignon) OCLCTIC
	9.3	Captation et diffusion d'images ou d'enregistrements portant atteintes à la vie privée	Art. 226-1 et 226-2 CP	VTN2 ou DCRI selon la nature des intérêts visés	OCLCTIC
	9.4	Atteintes au secret professionnel	Art. 226-13 CP	VTN2 ou DCRI selon la nature des intérêts visés	Variable selon contenu
Atteintes aux personnes	10.1	Vidéos de meurtres réels (snuff movies)	Art 221-1 et suivants CP	OCRVP ou Interpol	STRJD
	10.2	« Happy slapping » sans connotation xénophobe*	Art 222-33-3 CP	VNT1	
	10.3	Offense au chef de l'Etat	Art. 26 de la loi du 29 juillet 1881.	VTN2	
	10.4	Usurpation d'identité	Art. 434-23 CP	VNT1	
	10.5	Diffusion de montages sans consentement	Art. 226-8 CP	VTN1 ou 2 selon gravité	
	10.6	Exhibitionnisme *	Art. 222-32	VTN1	OCRVP
	10.7	Activités sectaires	Variable	VTN2	OCRVP DCRI SDIG (DCSP)
	10.8	Agences de casting illicites	Art. 227-22 CP si victimes mineures + infractions à l'agrément des agences	OCRTEH	PP (BPM) OCRVP
Atteintes à l'Etat et à la nation	11.1	Outrage à personne chargée d'un service public ou dépositaire de l'autorité publique	Art. 433-5 CP	VTN1 ou 2 selon la personne visée	Variable selon contenu
	11.2	Usurpation de fonction publique	Art. 433-13 CP	VTN1 ou 2 selon la personne visée	Variable selon contenu
	11.3	Atteintes au respect dû la Justice	Art. 434-25 CP	VTN1 ou 2 selon la personne visée	
	11.4	Provocation à l'espionnage ou à la trahison	Art. 411-11 CP	DCRI ou DPSD selon qu'il s'agit de civils ou de militaires	
	11.5	Provocation à la désobéissance	Art. 413-3 CP	DPSD (DGGN)	DCRI
	11.6	Vente d'uniformes et insignes des fonctionnaires participant au maintien de l'ordre	Décret-loi n°424 du 24/07/1944	VTN2	STRJD s'il s'agit de tenues militaires
	11.7	Atteinte au secret de la défense nationale	Art. 413-10 et suivants CP	DCRI	BLAT (DGGN) en cas de saisine d'une unité de gendarmerie UCLAT
Activités commerciales et professionnelles illicites	12.1	Exercice illégal de la médecine	Art. L 4161-5 du Code de la Santé Publique	VTN2	OCLAESP
	12.2	Exercice illégal de la pharmacie	Art L4223-1 du Code de la Santé Publique	VTN2	OCLAESP
	12.3	Usurpation de titre professionnel	Art. 433-17 CP	VTN2	Variable selon contenu
	12.4	Exercice illicite de la profession de banquier	Art. L511-5 et L571-3 du Code Monétaire et financier	VTN2	OCRGDF
	12.5	Infractions au code de la Consommation	Variable	DGCCRF	
	12.6	Infractions à l'éthique médicale	Art. 511-3 à 511-28 CP	VTN2	OCLAESP

Provocation au suicide	13.1	Provocation directe au suicide	Art. 223-13 CP	VTN1 (localisation de l'auteur de la provocation)	VTN1 (localisation de la personne provoquée au suicide)
	13.2	Apologie du suicide	Art. 223-14 et 223-15 CP	VTN2	SDIG (DCSP)
Infractions économiques et financières	14.1	Mise à disposition de programmes ou d'équipements permettant la falsification de moyens de paiement	Art. L163-4-1 Code Monétaire et financier	VTN2	OCLCTIC
	14.2	Sites de phishing	Incriminations diverses	VTN2	OCLCTIC
	14.3	Publicité et organisation de jeux, paris et loteries illicites	Art. 3 de la loi du 21 mai 1836 Loi du 12 juillet 1983 Loi du 2 juin 1891	SCCJ (DCPJ)	EM DRPJ Paris STRJD (DLCC) CYBERDOUANE DGCCRF
	14.5	Travail illégal	Art L. 324-9 du code du travail	VTN1 ou VTN2 selon ampleur	OCLTI (DGGN)
	14.6	Quêtes illicites	Art. 313-1 et 313-2-3° CP	VTN2	OCRGDF
	14.7	Publicité mensongère	Art. L.121-1 du Code de la Consommation	DGCCRF	OCRGDF
Traite des êtres humains	15.1	Proxénétisme	Art. 225-5, 225-6 et 225-7-10 CP	VTN2	OCRTEH
	15.2	Racolage	Art. 225-10-1 CP	VTN1	OCRTEH
	15.3	Trafics d'organes	Art. 511-2 s. CP	OCLAESP	OCRTEH
Réseaux d'immigration	16.1	Immigration irrégulière	Variable	VTN2	OCRIEST
Actes de cruauté envers les animaux	17.1	Sévices envers les animaux	Art. 521-1 CP	VTN1	
	17.2	Expérimentation illégale sur les animaux	Art. 521-2 CP	VTN2	OCLAESP
Divers	18.1	Dénonciations diverses *	Variable	Selon infraction et critères territoriaux	Variable selon contenu
	18.2	Spam (sans diffusion de documents pédophiles ni scam)	Art. 226-18 et 226-18-1 du Code Pénal Art. R10-1 du Code des Postes et des Communications Electroniques	Signal Spam	OCLCTIC si cela se rapporte à du phishing
	18.3	Urgence vitale (annonce de suicide ou de violences graves imminentes)	/	VTN1 par téléphone (CIC locale)	/
	18.4	Escroquerie en ligne	Art. 313-1 CP	VTN1 ou VTN2 selon ampleur (néant si le signalant est victime des faits)	OCLCTIC
	18.5	Utilisation frauduleuse de numéro de carte bancaire	Art. 313-1 CP	Pas de destinataire (information du public sur le portail)	/
	18.6	Outrage par utilisation du formulaire de signalement	Art. 434-24 CP	VTN1	/

	18.7	Injures et diffamations (sauf xénophobes)	Art. 32 al.2 et 33 al.3 de la loi du 29 juillet 1881	Pas de destinataire (information du public sur le portail)	/
	18.8	Fausse alerte / Fausse déclaration entraînant d'inutiles recherches	Art. 322-14 CP et 434-26 CP	VTN1 par téléphone (CIC locale)	VTN1 par téléphone
	18.9	Scam	Art. 313-1 CP	Pas de destinataire (information du public sur le portail)	OCLCTIC
	18.10	Signalements divers	Variable	Variable selon contenu	Variable selon contenu

Légende :

- **Domaine matériel** – Ce sont des domaines matériels que dépend la détermination des destinataires des signalements. Le domaine matériel est le plus petit élément statistique pris en compte par la plateforme. Il est distinct de la notion d'infraction : une même infraction peut se retrouver dans plusieurs domaines matériels, la référence matérielle permettant d'éviter toute confusion. Par exemple, les infractions de *diffusion de procédés permettant la fabrication d'engins explosifs* seront classées dans les catégories matérielles « terrorisme » ou dans « violences urbaines », en fonction du contexte des sites signalés.
- **Catégorie matérielle** – C'est un regroupement de domaines matériels proches. Ces catégories seront utilisées pour l'élaboration de statistiques globales. Cette classification sera propre à la plateforme de signalement et ne portera pas préjudice aux classifications statistiques utilisées par le ministère de l'Intérieur (STIC) et la DCPJ (Agora).
- **Référence matérielle « réf »** – Numérotation des domaines matériels
- **Source juridique** – C'est la source de la qualification juridique d'un contenu. Elle est communiquée aux services et unités destinataires d'un signalement.
- **Modes de saisine** – Pour attribution (destinataire unique pour chaque signalement) ou pour information (il pourra y en avoir plusieurs pour un même signalement).
- **Destinataires** – Pour chaque domaine matériel, une formule de détermination permet de désigner le destinataire d'un signalement : destinataire central – service ou unité spécialisé - ou ventilation territoriale (voir circulaire interministérielle et tableau en page 1 du présent)

* Remarques :

- **1.2 / 1.3 / 1.4 : provocations publiques à la haine et la discrimination** - la formule VTN1 sera privilégiée pour les provocations ponctuelles sur des forums publics ; la formule VTN2 sera privilégiée pour les contenus diffusés sur des sites spécialement conçus pour diffuser des contenus discriminatoires
- **1.5 / 10.2 : happy slapping** – Voir la catégorie « atteinte aux personnes » quand les violences ne présentent manifestement pas de caractère xénophobe
- **6.10 : autres contrefaçons (de marques...)** – Les services et unités servis pour information doivent se rapprocher au cas par cas pour convenir de l'attribution du signalement.

GLOSSAIRE

BLAT – bureau de la lutte anti-terroriste (DGGN)

CHEOPS – système de gestion des habilitations à l'accès aux fichiers informatiques de la Police Nationale

CIC – centre d'information et de commandement (DDSP)

CROGEND – centre de renseignement et des opérations de la gendarmerie nationale

CYBERDOUANE – cellule de lutte contre la fraude sur Internet.

DCPJ – direction centrale de la police judiciaire

DCRI – direction centrale du renseignement intérieur

DCSP – direction centrale de la sécurité publique

DDSP – direction départementale de sécurité publique

DGCCRF – direction générale de la concurrence, de la consommation et de la répression des fraudes

DIPJ – direction interrégionale de la police judiciaire

DLCC – division de lutte contre la cybercriminalité (STRJD)

DUTOP – division des unités territoriales et de l'ordre public (DCSP)

DPSD – direction de la protection et de la sécurité de la défense

DRD– direction du renseignement douanier

D3C– division ciblage et contrôle de la contrebande

DRPJ – direction régionale de la police judiciaire

« happy slapping » – violences commises dans le but d'être enregistrées et diffusées généralement sur Internet

IRCGN – institut de recherche criminelle de la gendarmerie nationale

MSN – Microsoft Network (logiciel de discussion en temps réel également appelé Microsoft Messenger)

OCLAESP – office central de lutte contre les atteintes à l'environnement et à la santé publique

OCLCO - office central de lutte contre le crime organisé

OCLCTIC – office central de lutte contre la criminalité liée aux technologies de l'information et de la communication

OCRGDF - office central pour la répression de la grande délinquance financière

OCRTEH - office central pour la répression de la traite des êtres humains

OCLTI – office central de lutte contre le travail illégal

OCRTIS - office central pour la répression du trafic illicite des stupéfiants

OCRVP – office central pour la répression des violences aux personnes

PHAROS – plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements

PP (BPM) – préfecture de police de Paris (brigade de protection des mineurs)

PROXIMA – système de gestion des habilitations à l'accès aux fichiers informatiques de la Gendarmerie Nationale

SCAEMS – section centrale armes, explosifs et matières sensibles (DCPJ)

SDIG – service départemental d'information générale STRJD – service technique de recherches judiciaires et de documentation

« tchat » – discussion écrite en temps réel entre deux internautes

UCLAT – unité de coordination de la lutte anti-terroriste

URL – uniform resource locator (lien indiquant l'accès à un contenu sur internet accessible par un logiciel de type « navigateur », commençant généralement par « http » ou « www »)