Les données de la délinquance

Partie A : Etat des lieux

1. Introduction

L'histoire de la France avec la transparence des données est toute particulière. Dès les années 70, le fichier SAFARI, ayant pour but de recouper les fichiers existants, afin de mieux connaître la population, crée la polémique. Le fichage a grande échelle, où tout serait interconnecté est vu comme une menace pour les libertés individuelles. De cette situation émerge la Commission Nationale de l'Informatique et des Libertés (C.N.I.L.) dont le rôle et d'encadrer la production, la conservation et l'utilisation de données, toujours plus importante, dans le respect des libertés de chaque citoyen. Avec l'entrée en vigueur du Règlement Général pour la Protection des Données (RPGD), le paradigme change. La protection des données se vit à l'échelle européenne et, comme nous le verrons dans un exemple concret, la CNIL voit son rôle évoluer.

Ces quarante dernières années la société a évolué vers toujours plus de technologies, plus précises, produisant des données massives. Dans un souci de transparence, et dans l'esprit de l'article 15[1] de la Déclaration des Droits de l'Homme et du Citoyen de 1789, les données produites par l'Etat doivent être rendues disponibles, accessibles et exploitables par tout citoyen.

Depuis 2011, l'Etat ouvre progressivement les données dont elle dispose et encadre cette ouverture grâce à de nouvelles lois. /…….

Pour que cette libération des données soit réellement pertinente et source d'innovation, il est nécessaire que le contenu mis à disposition soit fiable, le plus complet possible, récent, lisible, exploitable et ayant subi le moins de transformation possible.

Le but de cette ouverture, en plus de la transparence nécessaire au bon fonctionnement de la démocratie, est une meilleure efficience du service public, au travers du développement d'algorithmes intelligents, que se soit par des particuliers soucieux de s'investir dans ….., par des entreprises privées mieux à même de proposer des services et des technologies répondant aux besoins des services publics. Dans le domaine de la sécurité, cet enjeux semble capital.

2. La sécurité

[1] Article 15 : « la société a le droit de demander compte à tout agent public de son administration.

La criminalité est un sujet qui suscite l'intérêt. Pour preuve, entre 2012 et 2016, les données open data les plus téléchargées portaient sur ce sujet[2]. Ce dernier est principalement traité, de manières différentes, par le journaliste, le politicien et le citoyen.

Les journalistes n'ont pas un traitement « continu » de la criminalité, mais épisodique, faisant écho à l'actualité, dépourvu de contextualisation profonde. Les événements peuvent parfois y sont présentés de façon spectaculaire et dramatique, sous forme de faits divers « feuilletonnées ».

Sur la base de statistiques de faits criminels, rendues possible depuis la création de l'Etat 4001, indexant les crimes et délits par catégories et par commissariat, les politiciens ont la possibilité de développer des programmes politiques. Mais ces chiffres peuvent à la fois être présentés du point de vue national par le gouvernement, départemental par les députés ou encore communal par les maires. Tous ont raison, mais ne travaillant pas à la même échelle, cela peut vite devenir confus et finalement non représentatif de la vie ou du ressenti de chaque citoyen. Cette discordance de discours peut alors sembler contradictoire. Pour résumer, citons Boris Beaude : *« Ce constat questionne le traitement médiatique et politique de la criminalité qui, accordant une place importance à cette thématique, semble créer un décalage croissant entre la criminalité et sa perception* »[3]

3. <u>De quelles données, relative à la criminalité, dispose la France ?</u>

Les données utilisées sont généralement celles des services de sécurité (police, gendarmerie). Elles sont à la fois incomplètes – le chiffre noir de la délinquance, révélé par les enquêtes « cadre de vie et sécurité »[4] reste important – et ne correspond pas à la qualification pénale des faits et ne permet de connaître ni la sanction prononcée, ni celle effective. Pour se faire une représentation juste de la chaîne pénale, il faudrait ajouter les données issues des jugements. Depuis 1999, une partie de ces derniers sont accessibles en ligne sur le site légifrance.gouv.fr, sur le principe de publicité des décisions de justice (celle-ci est rendue au nom du peuple français et est publique)[5]

Bien que les décisions de justice soient accessibles, elles ne sont pour l'instant pas utilisées dans l'Open Data. Cela est dut en grande partie à la difficulté d'anonymisation complète et réellement des jugements[6]. L'ouverture de ces données ne doit permettre d'identifier ni les parties, ni les juges. Or, un recoupement de dates et de lieux pourrait lever l'anonymat des officiers de justice. Toutefois, ces données s'avèrent indispensable pour évaluer l'effectivité

[2]

[3] Boris BEAUDE « Crime mapping, ou le réductionnisme bien intentionné », EspacesTemps.net, (2009)

[4] Les enquêtes de victimisation ont pour but de révéler les faits de délinquance dont ont été victime les ménages et leurs membres. https://www.insee.fr/fr/metadonnees/source/serie/s1278

[5] http://www.justice.gouv.fr/organisation-de-la-justice-10031/les-fondements-et-principes-10032/la-publicite-des-decisions-de-justice-12037.html

[6] https://www.dalloz-actualite.fr/flash/open-data-des-decisions-de-justice-casse-tete-judiciaire-du-21e-siecle#.XHOeibjjKUk

de la réponse pénale, mais nous ne les inclurons pas dans notre étude, nous nous limiterons aux faits traités, ou non, par les forces de l'ordre.

Les dépôts de plaintes et constations policières, relatifs aux crimes et délits[7], sont collectés et classifiés dans l'Etat 4001. Ce fichier administratif, mis en place en 1972[8], comporte 107 index[9], que l'ONDRP[10] regroupe en 5 groupes qui sont : atteintes aux biens ; atteintes aux personnes ; infractions révélées par l'action des services (trafic de drogue, flagrants délits, etc.); escroqueries et infractions économiques et financières ; autres infractions.

Ce fichier est rempli par chaque commissariat, de police et de gendarmerie, présent sur le territoire. Le lieu des faits criminels n'est pas celui de « commission du crime » mais celui « d'enregistrement de la plainte ».

Il est possible de télécharger une version agrégée, donc non brute, de l'Etat 4001 sur le site Open data du gouvernement. Le traitement effectué préalablement à sa mise à disposition limite considérablement son exploitation. Par exemple, l'étude de ces données ne peut se faire qu'à l'échelle du département et non du commissariat, même si l'étude à l'échelle du commissariat pourrait faussée l'analyse car le dépôt de plainte peut se faire dans tous commissariats indépendamment du lieu de commission de l'infraction (un délit commis à Marseille peut être signalé et enregistré par la police d'Agen).

Les données issues de l'Etat 4001 sont souvent présentées sous formes statistiques mais également sous forme cartographique. Les statistiques peuvent être présentées aux citoyens par des organismes tels que l'INSEE ou l'ONDRP, au travers de revus, d'article, de lettres mais aussi par les journalistes et hommes politiques. Le politicien s'en sert pour argumenter son discours et justifier les décisions prises ou envisagées. Si l'ONDRP, l'INSEE et les journalistes peuvent revendiquer une certaine neutralité, pour l'homme politique cela semble plus difficile, les chiffres lui servent à présenter « une vérité » qui peut être orientée[11].

Même si actuellement la France n'ouvre pas toutes ces données criminelles au citoyen, elle les utilise quasiment en temps réel pour comprendre les phénomènes délinquants. Par exemple, à Carcassonne[12] où la représentation cartographique a montré une différence entre les lieux ayant mauvaise réputation et la réalité.

Ces données, une fois exploitées, permettent une meilleure compréhension du territoire pour les forces de l'ordre[13]. Elles devraient également être mise à disposition du citoyen pour qu'il se fasse une idée réaliste, et non imaginée, de la dangerosité de certains quartiers ou lieu. Or

[7] Les contraventions et mains courantes ne sont pas enregistrées dans l'Etat 4001.
[8] https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/024000053.pdf
[9] Index : la dénomination des infractions diffère de celle du système pénal, proche du vocabulaire usuel des policiers, mêlant des notions s'appliquant à l'acte et au mode opératoire.
[10] ONDRP : Observatoire National de la Délinquance et des Réponses Pénales
[11] https://www.lemonde.fr/societe/article/2011/01/20/la-delinquance-continue-a-baisser-mais-les-agressions-physiques-persistent_1468449_3224.htmlv
[12] https://www.ladepeche.fr/article/2011/02/16/1015358-carcassonne-la-cartographie-de-la-delinquance.html
[13] https://www.weka.fr/administration-locale/dossier-pratique/gerer-un-service-de-police-municipale-au-quotidien-dt29/la-cartographie-de-la-delinquance-6122/

dans ce domaine, que ce soit l'Etat, la région, le département ou la commune, aucun ne propose d'outil simple et pertinent sur ce sujet.

4. Qu'en est-il ailleurs dans le monde ?
    a. Aux Etats-Unis

Les états unis sont le pays pionner en matière d'utilisation des données de la délinquance et ce sous diverses formes et finalités. Le site adt.com/crime regroupe les crimes sur l'ensemble du territoire américain, mais il n'est pas le seul. Les polices des grandes villes possèdent leur propre système cartographique.

NEW-YORK[14]…….

LOS-ANGELES[15] met à disposition une carte de criminalité assez classique, où les délits sont répertoriés par catégories. Il est possible pour chaque citoyen d'y déclarer les crimes dont il a été témoin. Un filtre permet toutefois de n'afficher que ceux provenant des forces de police. Le site de la police de Los Angeles va plus loin en faisant la promotion de l'application « iWatch »[16] qui a vocation à « éduquer » les citoyens sur les comportements pouvant sembler criminels, notamment dans le cas de terrorisme et incite à « rapporter » tout comportement suspect. L'idée est que les forces de l'ordre et les citoyens peuvent et doivent travailler ensemble pour « protéger la collectivité ». Il est également possible de recevoir un courriel informant des faits criminels proche de chez soi. Ici, les données ne sont plus unilatérales mais bilatérales, avec tous les risques que cela peut engendrer, tel que des déclarations « abusives ».

    b. En Grande-Bretagne

LONDRES

Le cas de l'Angleterre a été étudié par l'ONDRP et présenté dans l'article « *De la fiabilité des statistiques de la criminalité enregistrée : le cas de l'Angleterre et du Pays de Galles* ». Y sont faites huit recommandations pouvant être appliquées aux données de type Open Data : « *l'information réponde aux attentes des utilisateurs* ; *l'impartialité et l'objectivité, ainsi que leurs processus de production, doivent être garanties* ; *l'intérêt public doit prévaloir sur l'intérêt personnel (politique institutionnel) et cela à tous les stades de production* ; *définir des règles méthodologiques, s'y tenir et les contrôler* ; *assurer la confidentialité des données (anonymisation)* ; *évaluer et équilibrer le ration coût-bénéfices* ; *assurer un financement permettant de garantir leur collecte et traitement* ; *rendre les données accessibles à tous en les accompagnant de commentaires clairs et exhaustifs* ».

    c. Au Canada

[14] https://data.cityofnewyork.us/Public-Safety/Crime-Map-/5jvd-shfj
[15] https://www.crimemapping.com/map/ca/losangeles
[16] http://www.lapdonline.org/iwatchla

Au Canada, il existe plusieurs modèles de mise à disposition des données appartenant au champ criminel.

OTTAWA[17], capitale du Canada, met à disposition ces statistiques dans un rapport[18] et utilise le même système cartographique[19] que les Etats-Unis. Elle met également à disposition de ces citoyens une application pour rester informé des actions de la police. De même, elle propose l'inscription à un courriel et propose de participer à la surveillance du quartier. Le citoyen est accouragé à agir pour prévenir le crime.

EDMONTON[20], permet la visualisation de 8 catégories de crimes (agressions, vols qualifiés, agressions sexuelles, homicides, entrées par effraction, vols de véhicules, vols de véhicules et vols de plus de 5 000 $). Il est précisé que 95,5% de ces crimes sont géolocalisés[21], mais qu'afin de préserver l'anonymat des victimes, les infractions figurent à « un bloc » du véritable lieu de commission. Les données sont issues des constations des policiers.

CALGARY[22] , dans un souci de transparence accrue, met à disposition une multitude de données concernant la ville. On peut y trouver des données criminelles mensuelles, fournies par les services de police, mais les types de crimes y figurants sont assez différents que ceux des villes précédemment étudiées. On y trouve de très nombreux types délinquances avec des informations sur l'état de l'auteur : « ivrogne, dérangement, loi sur la pudeur, plainte pour mineurs, propriétaire / locataire, problème de santé mentale, conflit de voisinage, plainte de partie, suspect, menaces, Drogues, Plainte pour bruit, coups de feu possibles, invité indésirable / mécène, prostitution, excès de vitesse, auto suspecte (regroupée en tant que désordre social), incendie, dommages à la propriété et auto abandonnée (regroupée dans un désordre physique) ».

SAINT JOHN[23], se réverse le droit de modifier les données après enquête, les crimes disponibles se limitent à l'effraction, le vol et le vandalisme[24]. Tout comme la ville de Ottawa, Saint-John propose à ses citoyens de s'inscrire à un courriel. Un outil interactif leur permet de « *créer eux-mêmes des rapports et d'observer des tendances* ».

Finalement, tous les modèles que nous avons vus sont très similaires. Les crimes y sont regroupés par catégories, il est possible de filtrer par date, de zoomer sur une rue, mais dans un souci d'anonymat, les infractions figurent à un bloc du lieu de commission. Les citoyens

[17] https://www.ottawapolice.ca/fr/index.aspx
[18] https://www.ottawapolice.ca/en/annual-report-2016/resources/2016/Crime-Trends-City-of-Ottawa-2016-2017.pdf
[19] https://www.ottawapolice.ca/en/annual-report-2016/resources/2016/Crime-Trends-City-of-Ottawa-2016-2017.pdf
[20] http://www.edmontonpolice.ca/CrimeFiles/NeighbourhoodCrimeMapping/HelpwithCrimeMapping
[21] http://crimemapping.edmontonpolice.ca/
[22] https://data.calgary.ca/Health-and-Safety/Community-Crime-Map/hhjd-wzc2
[23] http://www.saintjohn.ca/fr/Accueil/hoteldeville/servicesdeprotection/police/services/crimeprevention/crimemapping/default.aspx
[24] http://www.mapnimbus.com/DataNimbusClient.html?Client=City%20of%20Saint%20John#

peuvent parfois participer en rapport un fait délinquant dont ils ont été témoin, et dans presque tous les cas, l'individu peut être informé par mail de l'activité criminel existante dans son quartier. Bien plus qu'une simple mise à disposition des données, celles-ci sont mises en forme et destinées précisément aux habitants, voir même créées par eux.

5. Problématique

La France, en comparaison aux pays précédemment cités, accuse un sérieux retard tant dans la mise à disposition de données précises dans le domaine de la criminalité, que dans sa réutilisation. Alain Bauer, déclarait, en janvier 2018, qu' « *un logiciel de dépôt de plainte commun à la police, la gendarmerie et la Préfecture de police de Paris […] devra prendre en compte le lieu de commission du délit, et pas le lieu du dépôt de plainte, afin que la géolocalisation des infractions soit possible. »*[25] . Ce système permettra une harmonisation dans le recueil et le traitement des données.

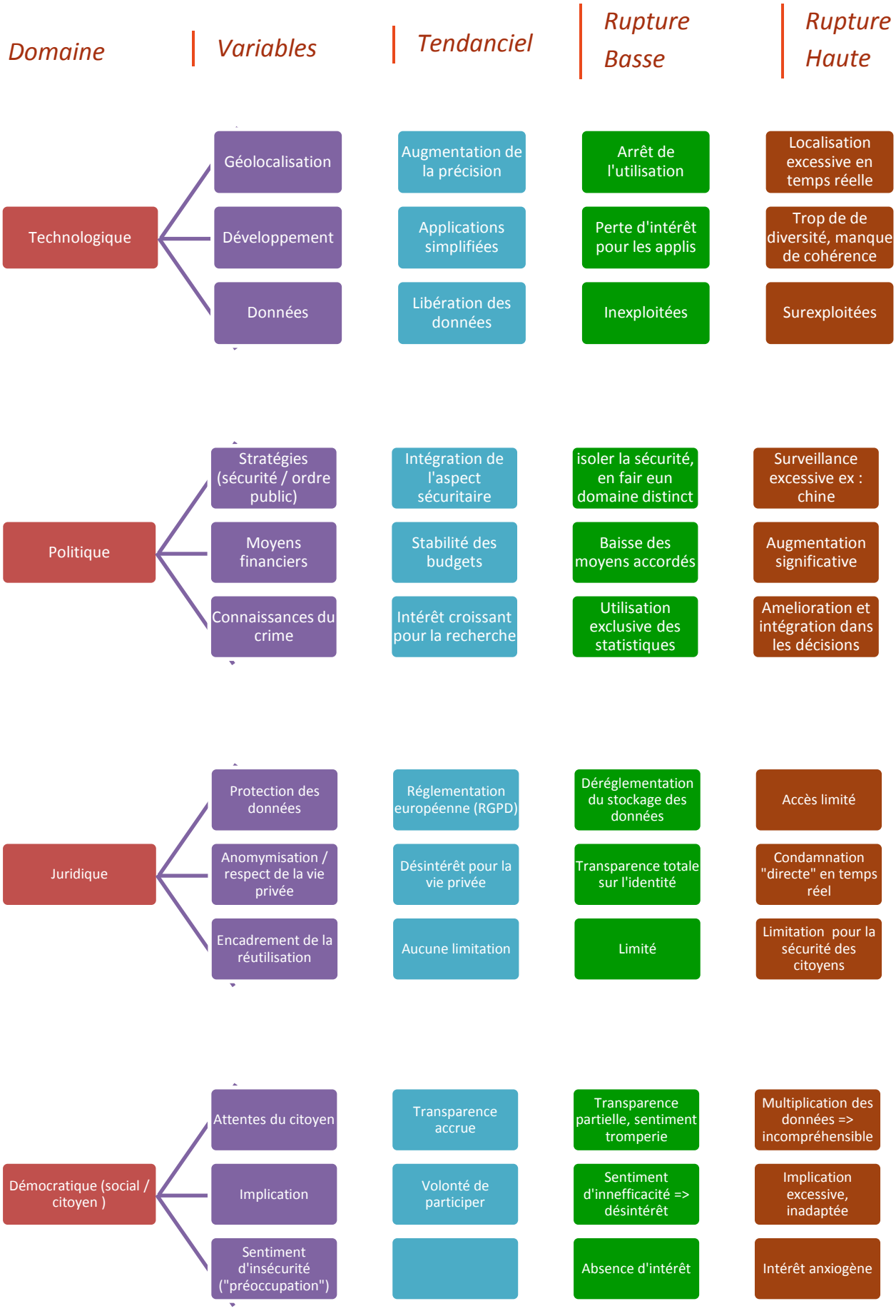
Une fois ce logiciel déployé, il faudra décider que faire des données criminelles géolocalisées obtenues. Doivent-elles être mise à disposition des forces de l'ordre seules ? Brutes ou retravaillées par un logiciel de type « PredPol[26] » ? Seront-elles ouvertes et accessibles aux citoyens ? Brutes ou agrégées ? Précisément géolocalisées, au risque de mettre en péril l'anonymat et la vie privée, ou « sectorisées » ? Quelle plus-value les entreprises privées pourraient-elles apportées à ces données ? En développant des applications, participatives ou non ? Est-ce que les risques de cette ouverture sont supérieurs aux bénéfices qu'elle apporte ? Faut-il inclure le citoyen dans la démarche ? Et si oui, jusqu'à quel point ?

Comme nous pouvons le voir, l'ouverture de données si précises sur la délinquance n'est que le début d'une succession de problématiques dont les politiques territoriales devront tenir compte et intégrer dans le développement de stratégies de politique publique et d'urbanisme.

Partie B : Etude Prospective Stratégique

Pour réaliser l'étude prospective stratégique, nous avons retenu 4 domaines : la technologie, la politique, la justice et la démocratie. Chaque domaine, ainsi eu son évolution possible, seront analysés suivant 3 variables, présentées dans le schéma suivant :

[25] https://www.lemonde.fr/idees/article/2018/01/05/le-crime-la-carte-et-le-territoire_5237721_3232.html
[26] https://www.predpol.com/


Domaine
Variables
Tendanciel
Rupture Basse
Rupture Haute
Technologique
Géolocalisation
Développement
Données
Augmentation de la précision
Applications simplifiées
Libération des données
Arrêt de l'utilisation
Perte d'intérêt pour les applis
Inexploitées
Localisation excessive en temps réelle
Trop de de diversité, manque de cohérence
Surexploitées
Politique
Stratégies (sécurité / ordre public)
Moyens financiers
Connaissances du crime
Intégration de l'aspect sécuritaire
Stabilité des budgets
Intérêt croissant pour la recherche
isoler la sécurité, en fair eun domaine distinct
Baisse des moyens accordés
Utilisation exclusive des statistiques
Surveillance excessive ex : chine
Augmentation significative
Amelioration et intégration dans les décisions
Juridique
Protection des données
Anomymisation / respect de la vie privée
Encadrement de la réutilisation
Réglementation européenne (RGPD)
Désintérêt pour la vie privée
Aucune limitation
Déréglementation du stockage des données
Transparence totale sur l'identité
Limité
Accès limité
Condamnation "directe" en temps réel
Limitation pour la sécurité des citoyens
Démocratique (social / citoyen)
Attentes du citoyen
Implication
Sentiment d'insécurité ("préoccupation")
Transparence accrue
Volonté de participer
Transparence partielle, sentiment tromperie
Sentiment d'innefficacité => désintérêt
Absence d'intérêt
Multiplication des données => incompréhensible
Implication excessive, inadaptée
Intérêt anxiogène

http://www.observatoire-des-territoires.gouv.fr/observatoire-des-territoires/fr/observatoire-national-de-la-delinquance-et-des-reponses-penales

1/ Scénario 1 : Ouverture totale non maîtrisée, réutilisation anarchique et nuisible

3/ Scénario 3 : Implication excessive et inadapté du citoyen

4/ Scénario 4 : Ouverture et réutilisation contrôlée : bonne connaissance du territoire, des événements criminels qui s'y déroulent mais protection du citoyen, pour éviter la révélation de l'identité des victimes et des auteurs.


Domaine
Variables
Tendanciel
Rupture Basse
Rupture Haute
Technologique
Géolocalisation
Développement
Données
Augmentation de la précision
Applications simplifiées
Libération des données
Arrêt de l'utilisation
Perte d'intérêt pour les applis
Inexploitées
Localisation excessive en temps réelle
Trop de de diversité, manque de cohérence
Surexploitées
Politique
Stratégies (sécurité / ordre public)
Moyens financiers
Connaissances du crime
Intégration de l'aspect sécuritaire
Stabilité des budgets
Intérêt croissant pour la recherche
isoler la sécurité, en faire un domaine distinct
Baisse des moyens accordés
Utilisation exclusive des statistiques
Surveillance excessive ex : chine
Augmentation significative
Amelioration et intégration dans les décisions
Juridique
Protection des données
Anomymisation / respect de la vie privée
Encadrement de la réutilisation
Réglementation européenne (RGPD)
Désintérêt pour la vie privée
Aucune limitation
Déréglementation du stockage des données
Transparence totale sur l'identité
Limité
Accès limité
Condamnation "directe" en temps réel
Limitation pour la sécurité des citoyens
Démocratique (social / citoyen)
Attentes du citoyen
Implication
Sentiment d'insécurité ("préoccupation")
Transparence accrue
Volonté de participer
Transparence partielle, sentiment tromperie
Sentiment d'innefficacité => désintérêt
Absence d'intérêt
Multiplication des données => incompréhensible
Implication excessive, inadaptée
Intérêt anxiogène

1/ Scénario 1 : Ouverture totale non maîtrisée, réutilisation anarchique et nuisible

Technologie : augmentation de la précision, trop de données sans réelle cohérence entre elles et surexploitées.

Politique : Utilisation des données sans recul, en les isolants des autres domaines sociaux et n'utiliser qu'elles pour définir une politique sécuritaire. => Idée fausse d'efficience (sur-efficience factice)

Juridique : Dérèglement du lieu et des moyens de stockage (pour faire baisser les coûts), données ouvertes à tous (et donc copiés et stockés par tous !!) et utilisation nombreuses tant par les citoyens que par les entreprises. (Possibilité de recouper de nombreuses données, menant à la disparition de l'anonymisation).

Démocratique : intérêt du citoyen mais multiplication des données mise à disposition au point d'être « noyé » (sentiment de confusion accrût), manque de compréhension ou interprétation fausse menant à un climat anxiogène.

Dans ce premier scénario, les données sont abondantes. Elles proviennent de tout appareil connecté pouvant être géo-localisé précisément et capable de produire des données relevant de la criminalité. Le manque de cohérence et d'interpolation rend flou l'exploitation judicieuse et l'anonymat n'est plus garantie.

Pourtant, le citoyen par sa volonté de participer s'emparer des données et cherche à les interpréter. Par manque de connaissance ou de recoupage avec les dispositifs mis en place, les politiques développées, l'exploitation peut être erronée, incomplète.

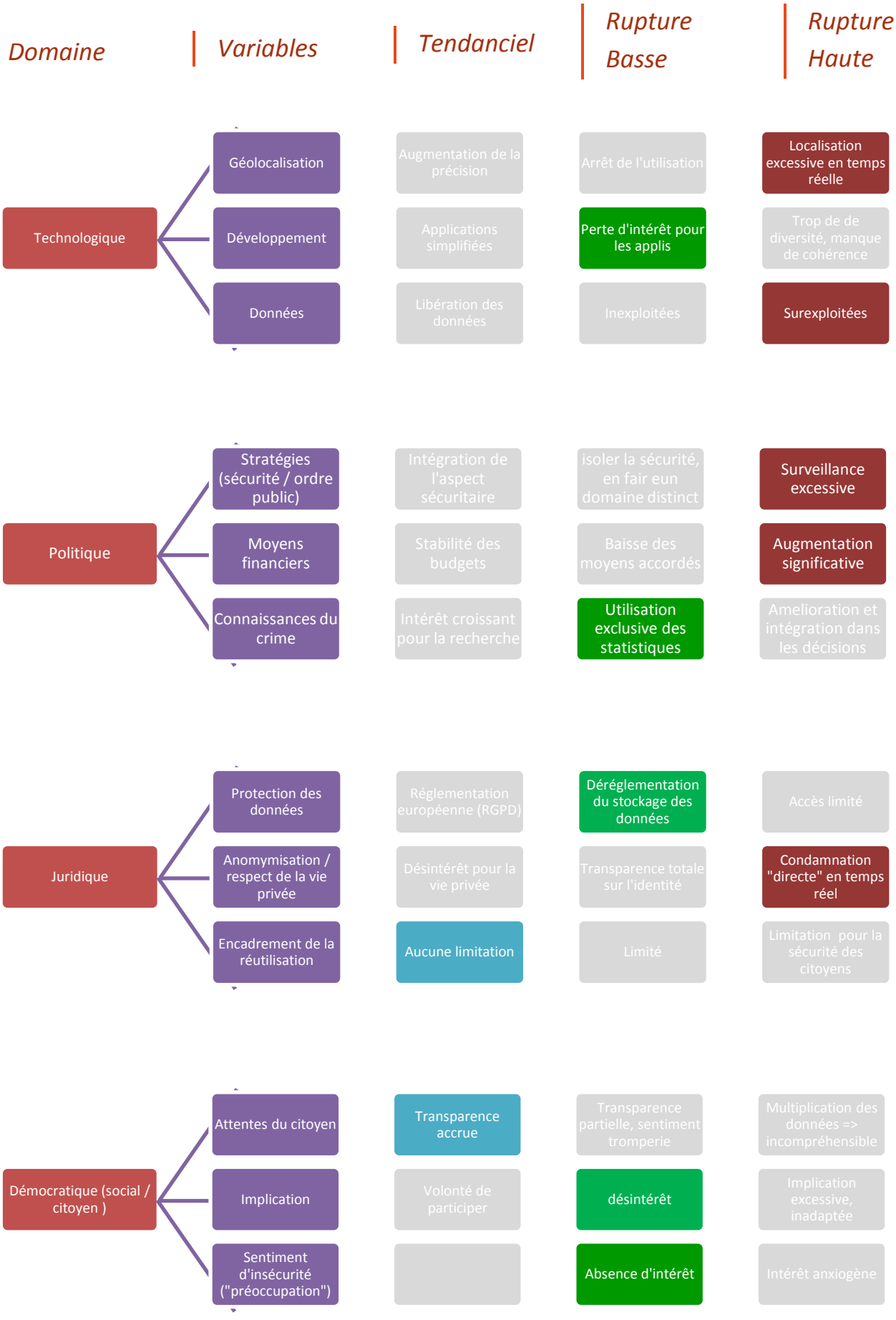
A l'ère des « fake news », la manipulation de données réelles, peut conduire à une distorsion de la vérité car l'information juste réside avant tout dans la présentation contextualisée et l'explication qui accompagnent les chiffres.

Autre possibilité, les signalements pourraient être « massivement faux ». En effet un moyen

Nice[27]

Crowdsourcing

[27] https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html


Domaine
Variables
Tendanciel
Rupture Basse
Rupture Haute
Technologique
Géolocalisation
Développement
Données
Augmentation de la précision
Applications simplifiées
Libération des données
Arrêt de l'utilisation
Perte d'intérêt pour les applis
Inexploitées
Localisation excessive en temps réelle
Trop de de diversité, manque de cohérence
Surexploitées
Politique
Stratégies (sécurité / ordre public)
Moyens financiers
Connaissances du crime
Intégration de l'aspect sécuritaire
Stabilité des budgets
Intérêt croissant pour la recherche
isoler la sécurité, en fair eun domaine distinct
Baisse des moyens accordés
Utilisation exclusive des statistiques
Surveillance excessive
Augmentation significative
Amelioration et intégration dans les décisions
Juridique
Protection des données
Anomymisation / respect de la vie privée
Encadrement de la réutilisation
Réglementation européenne (RGPD)
Désintérêt pour la vie privée
Aucune limitation
Déréglementation du stockage des données
Transparence totale sur l'identité
Limité
Accès limité
Condamnation "directe" en temps réel
Limitation pour la sécurité des citoyens
Démocratique (social / citoyen)
Attentes du citoyen
Implication
Sentiment d'insécurité ("préoccupation")
Transparence accrue
Volonté de participer
Transparence partielle, sentiment tromperie
désintérêt
Absence d'intérêt
Multiplication des données => incompréhensible
Implication excessive, inadaptée
Intérêt anxiogène

2/ Scénario 2 : Modèle vidéo-surveillance : Modèle chinois

Technologie : Localisation ultra-précise et en temps réel du délinquant, utilisé massivement par les forces de police, mais perte d'intérêt pour le développement de nouvelles applications ;

Politique : Forte augmentation des moyens alloués à la surveillance, partout et tout le temps, via l'implantation exponentielle de caméras ;

Juridique : Déréglementation du stockage et de l'exploitation des données au profit d'une sanction toujours plus rapide et visible ;

Démocratique : Transparence accrue mais une perte d'intérêt du citoyen car l'Etat est omniscient et omniprésent ;

Ici, la société est vue comme hyper-connectée et hyper-surveillée notamment grâce aux caméras de surveillance. Celles-ci représentent le meilleur moyen d'obtenir une multitude de données, géolocalisées, en temps réel, sur chaque citoyen et donc sur chaque fait criminel et les affaires traitées, les rapports établis par la police, le sont majoritairement à partir des faits criminels captés par les caméras.

Le scénario de l'utilisation jugée excessive des données criminelles peut se rapprocher du système mis en place actuellement en Chine. Les caméras de vidéo-surveillances sont omniprésentes, en 2016 il y en avait 176 millions soit plus de 3 fois plus qu'aux Etats-Unis, et dont 11% sont en lien avec une intelligence artificielle permettant la reconnaissance faciale[28]. Depuis le début de l'année 2018, les policiers sont mêmes équipés de lunettes-caméra là encore pour faciliter l'identification des individus.

Dans ce modèle, la condamnation est directe, en temps réelle, exemple du citoyen qui traverse en dehors du passage piéton et dont le visage apparaît sur un écran géant et qui a reçoit une amende. A première vue, ce système respecte parfaitement les 3 principes défendus par Beccaria concernant la justice qui, pour être efficace, doit appliquer une sanction « rapide, proportionnée et certaine ». Cela vaut pour les petites infractions mais devient moins efficace pour d'autres types de criminalités.

De plus, cette utilisation ne laisse que peu, voire pas du tout, de place au contradictoire. Tout comme l'ADN fût un temps jugé à tort comme une preuve « infalsifiable et sûre », les images vidéo peuvent être « mal » interprétées. Même si les caméras peuvent être trompées, avec du maquillage ou la dissimulation du visage, cela est très peu employé et surtout deviendra de plus en plus difficile avec le perfectionnement des technologies mises sur le marché.

Si ce modèle semble très tentant, il se nécessite un coût très élevé. L'achat, l'installation, l'entretien et l'exploitation des données…….

[28] https://www.ladepeche.fr/article/2018/10/08/2884060-videosurveillance-en-chine-un-systeme-a-grande-echelle.html

Enfin, cette organisation ne laisse plus de place au citoyen. Même si les données obtenues sont mises à la disposition du citoyen, cela n'a pas grand intérêt car les condamnations sont déjà effectives et rendues aux yeux de tous sans contradictoire. Le sentiment de « transparence » va au-delà de la transparence car chaque citoyen voit ses activités publiques enregistrées et scrutées en temps réel. Le contrôle social étant omniprésent et exercé par l'Etat, le citoyen peut se désengage totalement de l'aspect sécuritaire de la vie en collectivité. La transparence peut être réelle mais ne suscite aucun intérêt quant à l'exploitation, la réutilisation par le citoyen. Elle incite à un désengagement complet du citoyen.

En Chine, ce système a accru le sentiment de sécurité, 91% de la population se dit satisfait de la sécurité, et a fait baisser significativement la délinquance[29]. Ces résultats fûrent obtenu sans

La transparence est « excessive », elle n'assure aucune protection pour l'identité du délinquant et même de la victime. Cette première constatation ne semble pas compatible avec la volonté d'anonymisation qui existe dans la majorité des pays y compris la France. Ce modèle nécessite une confiance quasi-totale envers l'Etat, les moyens qu'il utilise et la manière dont il le fait. La multiplication exponentielle de caméras remet en cause la notion de vie privée.

Dans le département du Val-de-Marne[30], 31 communes sont équipées de caméras de vidéo-surveillance.

Transposition du modèle en France : situation de Villejuif avec une politique locale sécuritaire basée sur la multiplication des caméras de vidéosurveillances. Investissement important sur des lieux très ciblés mais difficultés, voir impossibilités de sécuriser les installations. Le poteau a était scié non pas une mais deux fois. Consultation publique des citoyens le 12 Janvier 2019. http://www.leparisien.fr/val-de-marne-94/villejuif-une-camera-a-reconnaissance-faciale-attaquee-a-la-disqueuse-22-10-2018-7924956.php

31 communes du val de marne équipées de caméras

Villejuif : demande aux locataires de payer pour sa sécurité privée (gardien de nuit dans l'immeuble) => refus par les locataires

Faut-il publier, rendre accessible tous les délits filmés ? Si oui, à quelles fins ? Appels à témoins donc participation du citoyen à la réalisation des crimes de proximité en temps réel ? Ou publication à titre informatif

Publication, mise à disposition des emplacements des caméras de vidéosurveillance : ex Agen https://www.data.gouv.fr/fr/datasets/cameras-de-video-protection/

http://oapi-fr.openstreetmap.fr/oapi/interpreter?data=node%5B%22man%5Fmade%22%3D%22surveillance%22%5D%3Bout%20body%3B%0A Indisponible

[29] http://french.china.org.cn/china/txt/2017-09/22/content_50023953.htm
[30] https://94.citoyens.com/2015/31-villes-du-val-de-marne-ont-installe-de-la-videosurveillance,05-02-2015.html

Les caméras sont référencées par les citoyens eux-mêmes https://www.camera-videosurveillance.fr/blog/47_TROUVEZ-LES-CAMERAS-PRES-DE-CHEZ-VOUS---.html
https://kamba4.crux.uberspace.de/?lat=48.7714153&lon=2.3469255&zoom=14

Sanction directe = effectivité de la justice, célérité de la réponse pénale (Beccaria)

Vidéosurveillance place le « flagrant délit » au centre de la réponse pénale.

Conclusion : Comme nous le montre les expériences citées au-dessus, un modèle reposant principalement sur la technologie, d'identification des délinquants, d'enregistrement en temps réel des crimes, ne peut être efficace que si elle est acceptée par la majorité des citoyens. Il faut qu'il y est une culture, un rapport à l'ordre, à la surveillance, biens particuliers.

Conclusion : si un modèle fonctionne très bien dans un pays, il n'est pas forcément transposable dans un autre. En France, la surveillance excessive ne semble pas être acceptée unanimement.

Partie C : Vers quel avenir se diriger ?

AVENIR DESIRABLE : Ouverture et réutilisation contrôlée : bonne connaissance du territoire, des événements criminels qui s'y déroulent mais protection du citoyen, pour éviter la révélation de l'identité des victimes et des auteurs.

Intégration du « sécuritaire » dans les domaines généraux (renforcement du tendancielle) ex : obligation du port de casque à moto fait baisser le vol à l'arraché.

Les données ont un réel impact sur l'évolution d'un quartier, au travers des infrastructures qui y seront construites, des investissements qui y seront fait ou non, des biens immobiliers qui peuvent chuter brutalement si le quartier semble dangereux

F. Furstenberg distingue dans le sentiment d'insécurité deux peurs, l'une qu'il désigne comme « personnelle », la seconde relevant de peur « sociale » qu'il nomme « préoccupation. Dans la peur personnelle, l'individu décrit plutôt l'état psychique dans lequel il se trouve. La « préoccupation » quant à elle se situe dans le registre « moral » et repose sur un « monde conçu ». Pour en parler, le citoyen utilise des phrases du type « il faut que » ou « il n'est pas acceptable que ». Pour diminuer cette peur, l'individu s'intéresse aux moyens utilisés pour assurer la sécurité.

L'ouverture des données de la criminalité pourrait permettre de maîtriser, rationnaliser, identifier ou mieux expliquer la « préoccupation » que ressent le citoyen et donc d'y répondre plus efficacement, en l'impliquant.

Meilleure connaissance des activités criminelles permet au citoyen de se prémunir plus efficacement, il devient actif de sa sécurité au lieu de ne compter que sur l'Etat et sa commune. Cette évolution est importante car la criminalité dépend beaucoup du milieu dans lequel elle évolue. De petits aménagements, peu coûteux mais bien penser peuvent avoir plus de bénéfices qu'une politique sécuritaire plus dure mais moins ciblée.

L'ouverture des données représente une reprise en main du domaine sécuritaire par le citoyen. Bien organisée, structurée et encadrée, elle peut éviter de créer un climat anxiogène et apporter une connaissance pertinente.

Si les nouvelles technologies, telle que les caméras de vidéosurveillances, doivent être mise en place, il faut qu'elles le soient intelligemment. Cibler massivement les quartiers à problèmes rend les dispositifs visibles, donc exposés aux dégradations et exacerbent le rejet. Les quartiers devraient voir leur sécurité traitée de la même manière. Ne pas se préoccuper

d’un quartier car il est actuellement non criminogène revient à préparer le terrain pour qu’une criminalité future s’y installe, s’enracine et se développe.