Kaléidos TRADUCTIONS

More than words

Mit der freundlichen Genehmigung vom Prof. Dr.-Ing. Ulrich Greveler	Avec l'aimable autorisation du Prof. Dr.-Ing. Ulrich Greveler
Freiheit, Informationssicherheit oder Datenschutz: Müssen wir uns entscheiden?[1]	**Liberté, sécurité de l'information ou protection des données : faut-il vraiment choisir ?[1]**
Ulrich Greveler Fachhochschule Münster, Labor für IT Sicherheit, 48565 Steinfurt greveler@fh-muenster.de	Ulrich Greveler Fachhochschule Münster, Laboratoire de sécurité informatique, 48565 Steinfurt (Allemagne) greveler@fh-muenster.de
Zusammenfassung	**Résumé**
Das Prinzip aus dem Datenschutzrecht bekannte der „Datensparsamkeit und Datenvermeidung" wird technisch um das Konzept des „irreversiblen Verschlusses" erweitert. Daten können unter Nutzung vertrauenswürdiger Hardware in einer Weise gespeichert werden, die zwar eine Verarbeitung für bestimmte Zwecke erlaubt, ein Abrufen des vollständigen Datenbestandes jedoch zuverlässig verhindert. Die verschlossenen Daten, die vorzugsweise bei einem öffentlich bestelltem, unabhängigen Datenspeicherer gespeichert und verarbeitet werden, stehen dann keiner Partei mehr zur Verfügung, wodurch insbesondere eine unrechtmäßige vorsätzliche oder fahrlässige Weitergabe des Datenbestandes verhindert wird. Der Beitrag beschreibt das Konzept und stellt mögliche Anwendungsfälle in einem Gedankenexperiment vor, dass anlässlich der MinD-Akademie 2009 in Nürnberg diskutiert wurde.	La technique du « chiffrement à sens unique » prolonge le principe de limitation de la collecte issu du droit à la protection des données. L'utilisation d'un matériel de confiance autorise le traitement des données pour une finalité déterminée, mais garantit l'inviolabilité de l'accès à l'ensemble des données enregistrées. Dans le meilleur des cas, un organisme neutre, compétent et indépendant procède à l'enregistrement et au traitement des données. Dès l'instant où les données sont chiffrées, aucune des parties ne peut plus y accéder. Le transfert non autorisé des données – que ce soit un acte malveillant ou une erreur –, est ainsi empêché. L'article décrit cette technique et envisage d'éventuelles applications à travers une expérience de pensée, débattue lors de la conférence MinD-Akademie en 2009 à Nuremberg.
Fußnote	**Note de bas de page**
[1]Der Beitrag stellt eine geringfügig aktualisierte Version der Publikation Irreversibler Verschluss: DRM-basierter Datenschutz des Autors, erschienen in Patrick Horster (Hrsg.), D.A.CH Security '09, syssec, ISBN 978-3-00027-488-6, dar.	[1] Cet article est une version résumée et actualisée de l'ouvrage du même auteur : *Chiffrement à sens unique : des DRM pour protéger les données personnelles* (Titre de l'original : *Irreversibler Verschluss: DRM-basierter Datenschutz*), Patrick Horster (dir.), D.A.CH Security '09, syssec, ISBN 978-3-00027-488-6.

1 Einführung	**1 Introduction**
Wir skizzieren die Entwicklung einer datenschutzfördernden Technologie auf Basis digitaler Rechteverwaltung. Der technologische Ansatz besteht darin, eine Speicherung sensibler Daten in einer Weise vorzusehen, dass sie „für immer verschlossen“ bleiben, auch aus Sicht der Partei, die die Datenspeicherung vornimmt.	Nous allons décrire la mise au point d'une technologie respectueuse de la protection des données, basée sur la gestion des droits numériques. Notre approche technologique consiste à enregistrer les données sensibles de manière à ce qu'elles restent « définitivement chiffrées », y compris pour l'autorité qui a procédé à leur enregistrement.
Die Kernidee kann in folgende Aspekte aufgeteilt werden.	Ce concept clé repose sur les principes suivants :
• Das Prinzip der „Datensparsamkeit und Datenvermeidung“ wird technisch um das Konzept des „irreversiblen Verschlusses“ erweitert. Wir entwickeln ein System, das zweckgebundene Daten einerseits speichert, sie aber andererseits nie mehr unverarbeitet preisgibt, so dass bei vorsätzlichem wie fahrlässigem Fehlverhalten ein Missbrauch ausgeschlossen wird und die Zweckbindung der Datenhaltung technisch erzwungen wird.	• La technique du « chiffrement à sens unique » représente une avancée au regard du principe de limitation de la collecte. Nous développons un système capable d'enregistrer les données collectées dans un but précis, tout en ne donnant ensuite plus jamais accès aux données brutes. Ainsi, l'utilisation illicite des données, due à une erreur de manipulation ou à un acte de malveillance, est exclue. La finalité de la conservation des données est techniquement contrainte.
• In einem Gedankenexperiment überlegen wir, inwieweit die Existenz einer solchen Technologie rechtfertigen würde, beliebige personenbezogene Daten „auf Vorrat“ zu speichern, ohne die derzeit im Datenschutzrecht vorgesehenen Einschränkungen (Zweckbindung, Zustimmungsvorbehalt) vorzusehen. Die Datenspeicherung würde dann grundsätzlich alle(!) anfallenden personenbezogenen Daten umfassen.	• À travers une expérience de pensée, nous cherchons à comprendre dans quelle mesure cette technologie, si elle était au point, pourrait justifier l'enregistrement et la conservation de grandes quantités de données personnelles, sans pour autant devoir tenir compte des limites actuelles du droit à la protection des données (principes de finalité et de consentement préalable). Ainsi, en théorie, l'enregistrement pourrait concerner toutes (!) les données personnelles accumulées.
• Die Datenspeicherung erfolgt (innerhalb des Gedankenexperiments) nicht mehr bei der erhebenden Partei (z. B. Unternehmen, das Kundendaten speichert) sondern allein bei einem öffentlich-rechtlich bestellten, von wirtschaftlichen Interessen der erhebenden Partei unabhängigen Datenspeicherer, der allein dem Gesetz verpflichtet ist (im weitesten Sinne vergleichbar mit dem derzeitigen Datenschutzbeauftragten). Ein Zugriff auf diese Daten bzw. die Verarbeitung der Daten (insbesondere Ablgeich zwischen Datenbeständen) erfolgt dabei zwingen unter Benachrichtigung der Betroffenen (hier: Subjekt, auf das sich das jeweilige personenbezogene Datum bezieht).	• Dans le cadre de cette expérience, ce n'est plus le responsable de la collecte (par ex. l'entreprise qui enregistre les données de ses clients) qui procède à l'enregistrement des données, mais un organisme neutre, compétent, financièrement indépendant et unique responsable devant la loi (à l'image de l'actuel délégué à la protection des données personnelles, homologue du correspondant informatique et libertés en France). Les personnes concernées (ici, l'individu à qui appartient chacune des données) doivent être informées lorsque leurs données sont consultées ou font l'objet d'un traitement (en particulier en cas de rapprochement avec d'autres bases de données).

Ein System, dessen Architektur in diesem Beitrag skizziert wird, stellt folgende Funktionen bereit:	Le système basé sur l'architecture présentée dans cet article propose les fonctions suivantes :
• Datenhaltung großer Datenmengen, die nicht ausgegeben werden, jedoch für definierte Prozesse (z. B. einmalige Auswertung) zur Verfügung stehen	• stockage d'importantes masses de données, non consultables, auxquelles seuls des processus spécifiques ont accès (par ex. dans le cas d'un accès unique aux données)
• Rechteverwaltung für Datenobjekte und Nutzer bzw. Rollen	• gestion des droits applicables aux données objets et aux utilisateurs ou statuts ;
• Datenabgleiche von externen mit internen Daten bzw. zwischen internen Daten verschiedener Systeme, wobei nur die „Treffer" im Detail (in vorbestimmter Maximalzahl) oder als Anzahl ausgegeben werden und die Art des Abgleichs aus einer weißen Liste erlaubter Operationen zu wählen ist	• rapprochements de données internes et externes ou rapprochements des données issues de différents systèmes, à condition de ne consulter qu'un nombre (limité et fixé à l'avance) de résultats correspondants à la recherche, en clair ou sous forme chiffrée. Le mode de rapprochement utilisé doit figurer sur une liste d'opérations autorisées (liste blanche) ;
• Gewinnung statistischer Aussagen über die Gesamtheit des Datenbestandes	• génération de rapports statistiques portant sur l'ensemble des données enregistrées ;
• Beweissichere Protokollierung der Operationen auf dem Datenbestand	• protocole de sécurisation des opérations effectuées sur l'ensemble des données enregistrées ;
• Zwingende Information der betroffenen Personen bei Zugriff auf Datenbestand bzw. Verarbeitung personenbezogener Daten	• obligation d'informer les personnes concernées en cas de consultation des données enregistrées ou en cas de traitement des données personnelles.
Anwendungsfelder sind hier Datenabgleiche zwischen Behörden (z. B. Identifizieren von Personen, zu denen Daten im Bestand mehrerer Behörden vorliegen), die auf klar definierter gesetzlicher Grundlage erfolgen, wobei vermieden werden soll, dass beteiligte Mitarbeiter den Gesamtdatenbestand einsehen, drucken, erheblich modifizieren, versenden oder elektronisch auf Datenträger kopieren können.	Cette technique s'applique dans le domaine des rapprochements de bases de données publiques (par ex., pour identifier des personnes dont les données se trouvent dans les bases de plusieurs administrations). Ces rapprochements sont juridiquement très encadrés, ce pour éviter toute consultation, impression, modification importante, envoi ou copie sur un support électronique de l'ensemble des données enregistrées par un des collaborateurs impliqués dans cette opération.

1.1 „Datenpannen“ in der jüngeren Vergangenheit	**1.1. Affaires récentes de « perte de données »**
In jüngster Zeit gab es einige Datenschutzverletzungen, die ein beträchtliches Medienecho (Skandale um sog. „Datenpannen“) auslösten. Beispielhaft seien die folgenden genannt.	Une série d’atteintes à la protection des données personnelles (« affaires des pertes de données ») a récemment fait la une des médias allemands. Parmi elles, on peut citer les suivantes :
• Am 4.10.2008 wurde gemeldet, dass beim Netzbetreiber *T-Mobile* bereits im Jahre 2006 mehr als 17 Millionen Kundendatensätze kopiert und „am Schwarzmarkt angeboten“ wurden.	• Le 4 octobre 2008, la découverte de la copie et de la mise en vente, sur le marché noir, dès 2006, de 17 millions de données clients détenues par l’opérateur réseau T-Mobile.
• Die *Deutsche Telekom* hat in den Jahren 2005 und 2006 durch ein Berliner Beratungsunternehmen Telefonverbindungsdaten eigener Manager und von Aufsichtsräten der Arbeitnehmerseite auswerten lassen.	• De 2005 à 2006, l’opérateur allemand Deutsche Telekom fait analyser par une société de conseil berlinoise les enregistrements des conversations téléphoniques de ses propres cadres, de représentants de son personnel et des membres de son conseil de surveillance.
• Im Dezember 2007 wurde bekannt, dass in Großbritannien die gespeicherten Namen, Anschriften und E-Mail-Adressen von rund drei Millionen Führerscheinanwärtern mit dem Datenträger „verloren“ wurden. [Netz07]	• En décembre 2007, on apprend qu’en Grande-Bretagne, les noms, adresses et e-mails contenus dans le fichier recensant les près de trois millions de candidats au permis de conduire ont été « égarés ». [Netz07]
• Im September 2008 räumte die Hochschulleitung der Universität Göttingen ein, dass die Daten von 26.000 Studenten ungeschützt auf einem Internetserver zugänglich waren. [Unis08]	• En septembre 2008, la direction de l’université de Göttingen reconnaît que les données de 26 000 étudiants n’ont pas été protégées et sont accessibles via un simple serveur Internet. [Unis08]
Die Liste ließe sich fortsetzen; in der Zeit zwischen der Einreichung dieses Beitrages und der Fertigstellung der Druckversion haben sich weitere öffentlich wahrgenommene Fälle (z. B. *Deutsche Bahn*) ereignet. Obwohl diese Skandale unterschiedlicher Natur sind (Vorsatz versus Fahrlässigkeit), gibt es eine Gemeinsamkeit: Die entwichenen Daten wurden offenbar nicht in technischer Hinsicht ausreichend geschützt, obwohl es anwendbare Technologien und Verfahren gibt. „Skandalös“ aus technischer Sicht ist, dass die „Datenpannen“ möglich waren, unabhängig davon, dass es zudem ein juristisch zu bewertendes Fehlverhalten gab.	La liste pourrait être encore longue : entre le moment où cet article a été rédigé et l’impression de la version définitive, d’autres exemples ont fait irruption dans le débat public (par ex., celui de la *Deutsche Bahn*, l’entreprise ferroviaire publique allemande). Bien que d’origine différente (malveillance *vs.* erreur), ces affaires ont toutes un point commun : les données disparues n’étaient manifestement pas assez protégées sur le plan technique, alors que des technologies et des procédures peuvent être appliquées. Au-delà du caractère juridiquement répréhensible de ces actes, on ne peut accepter sur le plan de la technique que ce type de « pertes » se produise.

2 Stand der Technik, bisherige Arbeiten	**2 État de la technique et travaux réalisés à ce jour**
Für die Architektur der Plattform ausschlaggebend ist der Stand der Technik in Bezug auf vertrauenswürdige Hardware und Trusted Computing. 2003 wurde von führenden IT-Unternehmen eine gemeinnützige Organisation gegründet, die offene Standards für sichere Hardware- und Softwareprodukte erarbeiten soll. Unter dem Namen Trusted Computing Group (TCG) versuchen die beteiligten Unternehmen, ihre Sicherheitsinitiativen zu koordinieren. Den Kern der Arbeit der TCG bildet die Spezifikation eines Moduls, auf dem das gesamte Sicherheitskonzept aufbaut: das Trusted Platform Module (TPM). Das TPM ist ein passiver Chip, der einen Mikrokontroller enthält und fest mit dem Mainboard oder dem Prozessor verbunden ist. Es ist von seiner Architektur her mit einer Prozessorchipkarte vergleichbar. Wesentliche Funktionen des TPM sind die Bereitstellung eines speziellen Schlüssels, mit dem die Plattform von Dritten als vertrauenswürdig erkannt werden kann, und die sichere Erkennung einer als vertrauenswürdig angenommenen Systemkonfiguration.	L'état de la technique s'agissant du matériel de confiance (*Trusted Hardware*) et de l'informatique qui lui est associée (*Trusted Computing*) conditionne l'architecture de la plateforme. En 2003, d'importantes entreprises du secteur informatique ont créé une organisation à but non lucratif chargée de définir des standards ouverts améliorant la sécurité des produits matériels et logiciels. Ces entreprises, réunies au sein du groupe TCG (*Trusted Computing Group*), s'efforcent de coordonner leurs initiatives en faveur de la sécurité. Le travail du TCG consiste pour l'essentiel à définir la spécification d'un composant sur lequel repose l'intégralité du dispositif de sécurité : le module de confiance de plate-forme (en anglais : *Trusted Platform Module* [TPM]). Le TPM est une puce électronique passive, qui contient un microcontrôleur relié à la carte mère ou au processeur. Son architecture est identique à celle d'un processeur. Le TPM a pour principales fonctions la génération d'une clé spéciale qui permet à la plateforme d'être identifiée comme un tiers de confiance, ainsi que la reconnaissance sécurisée des configurations de système jugées dignes de confiance.
Digitale Rechteverwaltung (DRM) bezeichnet Verfahren, mit denen Verbreitung und Nutzung digitaler Inhalte gesteuert und überwacht werden soll. Die unter DRM gefassten Technologien wurden ursprünglich für audiovisuelle Medien und Rundfunkübertragungen konzipiert (Scrambling, DVD, PayTV u. a.), können aber zum Teil auf beliebige Daten in digitaler Form angewandt werden. Ausnahmen stellen forensische Verfahren wie digitale Wasserzeichen dar, die auf starke Redundanz zu schützender Daten abzielen, die außerhalb des audiovisuellen Bereiches allgemein nicht gegeben ist.	La *gestion des droits numériques* (DRM) désigne les procédés permettant de contrôler et de surveiller la diffusion et l'utilisation de contenus numériques. À l'origine, les technologies DRM ont été développées pour les contenus audiovisuels et radiodiffusés (notamment le cryptage des DVD et de la télévision payante), mais certaines peuvent aussi être utilisées avec de nombreux autres types de données sous forme numérique ; font exception les procédés légaux tels que les tatouages numériques, basés sur la forte redondance des données à protéger – une caractéristique propre au domaine de l'audiovisuel.

Während im Sektor PayTV (Bezahlfernsehen) seit den 80er Jahren DRM (und seine Vorläufer) ein erfolgreiches Geschäftsmodell für Multimedia-Inhalte trotz der zunehmenden Digitalisierung der Fernseh- und Filmproduktionen auf der einen Seite und verbesserter Multimediafähigkeit von Privatanwender-PCs auf der anderen Seite ist, scheiterte die Verwendung von DRM beim Vertrieb von Musikstücken und Datei-Downloads. Als Ursache wird meist eine mangelnde Akzeptanz beim Verbraucher angenommen, der – wenn er zur Nutzung von DRM gezwungen wird – den Konsum DRM-geschützter Stücke als unpraktisch und übertrieben restriktiv empfindet bzw. berechtige Sorge haben muss, dass der zukünftige Konsum bei Neuanschaffung von Nachfolgegeräten nicht mehr möglich ist. Ein freier Datenfluss wird durch DRM allgemein verhindert; diese Eigenschaft ist für die in diesem Beitrag beschriebene Anwendung jedoch nicht nachteilhaft, sondern wird ausgenutzt.	Depuis les années 1980, les DRM (et les systèmes qui les ont précédées) constituent un modèle économique viable pour la diffusion de contenus multimédias dans le domaine de la télévision payante. Et ce, alors que les productions pour la télévision ou le cinéma sont de plus en plus numérisées et que la puissance des ordinateurs des particuliers s'est améliorée. À l'inverse, l'utilisation des DRM dans le cadre de la vente de musique et du téléchargement de fichiers a été un échec. L'explication la plus couramment admise est qu'elles sont peu appréciées par l'utilisateur. Celui-ci, lorsqu'il est obligé d'utiliser cette technologie, a en effet le sentiment que consommer de la musique protégée par un DRM est peu pratique et exagérément restrictif. De plus, son inquiétude de ne plus pouvoir utiliser le produit s'il s'équipe de lecteurs de nouvelle génération est fondée. En général, les DRM bloquent la libre circulation des flux de données. Néanmoins, cette caractéristique n'est pas un obstacle à l'application décrite dans cet article, elle sera au contraire un facteur de facilitation.
Rechtebeschreibungssprachen dienen der Kodierung von Rechtebeschreibungen in maschinenlesbarer Form. Unter Rechtebeschreibung (Rights Expression) wird im hier betrachteten Umfeld eine formale Beschreibung verstanden, die ausdrückt, dass einem bestimmten Nutzer (bzw. einer Rolle) ein Recht gewährt oder entzogen wird, unter gewissen Bedingungen eindeutig beschriebene Datenfelder auf eine festgelegte Art und Weise zu nutzen. Die Rechtebeschreibung stellt daher ein formalisiertes Einzelrecht, d. h. eine Zuordnung dieser (max). fünf Objekte untereinander dar. Die für die Plattform interessanten Sprachen sind die XMLbasierten Konstrukte Security Assertion Markup Language (kurz SAML), Open Digital Rights Language (ODRL) und eXtensible Access Control Markup Language (XACML). Insbesondere ODRL erscheint für Implementierungen in besonderer Weise geeignet, da es dokumentierte Erfahrungen in der DRM-Anwendung von ODRL und Open-Source-Implementierungen des Interpreters gibt.	Les *langages d'expression des droits* sont utilisés pour développer le code informatique servant à décrire les droits. L'expression des droits (*Rights Expression*) correspond dans ce contexte précis à la description formelle d'une procédure d'attribution ou de déni d'un droit (ou statut) en fonction d'un utilisateur donné. Le cas échéant, il pourra utiliser sous certaines conditions et selon des règles préalablement établies des champs de données clairement définis. L'expression des droits équivaut ainsi à la formalisation d'un droit individuel correspondant à l'allocation successive de cinq attributs (au maximum). Les langages reconnus par la plateforme sont les structures basées sur XML : *Security Assertion Markup Language* (sigle : SAML), *Open Digital Rights Language* (ODRL) et *eXtensible Access Control Markup Language* (XACML). ODRL semble particulièrement adapté aux développements, en effet il existe des expériences documentées sur l'utilisation du langage ODRL appliqué aux DRM, ainsi que sur les développements open source conformes à ce langage de programmation.

2.1 Ansätze zur Nutzung von DRM für den Datenschutz	**2.1. Approches de la protection des données par l'utilisation de DRM**
Eine Nutzung von DRM-Technologie zum Schutz personenbezogener Daten wird von Böhme und Pfitzmann [BöPf08] kritisch betrachtet. Die Autoren weisen darauf hin, dass DRM für Medieninhalte sehr fehleranfällig sei und dass Privacy-DRM unter technisch deutlich ungünstigeren Voraussetzungen noch höhere Anforderungen erfüllen müsse. Zudem könnten digitale Wasserzeichen, eine Kerntechnologie heutiger Medieninhalte-DRM-Technik, für Privacy- DRM praktisch nicht eingesetzt werden. Es wird gefolgert, dass Privacy-DRM grundsätzlich anders realisiert werden müsse, nämlich unter Einsatz von manipulationssicherer vertrauenswürdiger Hardware.	R. Böhme et R. Pfitzmann mettent en garde contre une utilisation de la technologie DRM à des fins de protection des données personnelles. Les auteurs montrent que les DRM appliquées aux contenus multimédias sont instables et qu'elles doivent répondre à des exigences plus élevées en raison de conditions techniques beaucoup moins favorables à la vie privée. De plus, la technique ne permet pas d'incruster les tatouages numériques – une technologie aujourd'hui au cœur des DRM, utilisée pour la gestion de contenus multimédias – dans les DRM destinées à protéger la vie privée (en anglais, *Privacy-DRM*). Par conséquent, ce type de DRM doit être mis en œuvre autrement, à savoir au moyen d'un matériel de confiance qui sécurise davantage les opérations.
Beim zweiten Internet Governance Forum (IGF) der UN gab es für die Idee des Persönlichen DRM Zustimmung: Simon Davies, Direktor der Organisation Privacy International (PI), sprach sich dafür aus, in Zukunft auf technische Lösungen zu setzen: „Es ist klar, dass rechtliche und Marktlösungen nicht in ausreichendem Maß den individuellen Nutzer in seinen Rechten schützen können, daher müssen wir einen Weg einschlagen, der Nutzerkontrolle durch technische Infrastrukturen einbezieht" [Davi07].	Lors du deuxième Forum sur la gouvernance de l'Internet (FGI) organisé par l'ONU, un consensus s'est formé autour de l'idée de DRM personnelle : Simon Davies, directeur de l'organisation *Privacy International* (PI), s'est déclaré favorable à la perspective du déploiement de solutions techniques : « Il est clair que les solutions juridiques et d'auto-régulation ne permettent pas de protéger suffisamment les droits de l'utilisateur, c'est pourquoi nous devons nous orienter vers un contrôle de l'utilisateur par les infrastructures techniques. » [Davi07]
Schallaböck vom unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) weist darauf hin, dass DRM in der (i. a. kritisch vorgenommenen) Interpretation als Digital Restrictions Management gerade für den technischen Schutz personenbezogener Daten geeignet sei, da diese nicht dem Free Flow of Information unterliegen sollten und die technische Durchsetzung der Zweckbindung erhobener Daten eine DRM-Infrastruktur nahe lege [Scha06].	J. Schallaböck, du centre indépendant pour la protection des données du Land de Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz* − ULD), affirme que les DRM, interprétées (souvent en mauvaise part) comme un système de « gestion des restrictions numériques », sont justement adaptées à la protection technique des données personnelles, car elles ne seraient pas soumises au libre flux d'information. La contrainte de finalité des données exigerait une infrastructure DRM [Scha06].
Die Verwendung von Trusted-Computing-Technologie (hier: TCPA[2]) zur Duchsetzung digitaler Rechte ist Gegenstand zahlreicher Veröffentlichungen [Eric03, GSS03, ReCa05]. Datenschutzaspekte in Bezug auf diese Technologie werden meist kritisch [Bech05] betrachtet oder die Technologie wird in Gänze als gesellschaftliche Gefahr wahrgenommen und verworfen [Gras06]. So schreibt bereits im Jahre 2003 Roy Pfitzner (beim Landesbeauftragten für den Datenschutz Brandenburg): „TCPA wurde oft mit einem datenschutzunfreundlichen DRM Betriebssystem gleichgesetzt. Fehlerhafte Darstellungen zu der TCPA-Technologie haben ihren Eingang in	De nombreuses publications portent sur l'utilisation de technologies d'informatique de confiance (conformes aux spécifications de la TCPA[2]) pour la mise en place de droits numériques [Eric03, GSS03, ReCa05]. Ces technologies sont en grande partie critiquées pour leur gestion de la protection des données ou encore rejetées, car elles sont globalement perçues comme une menace pour la société [Gras06]. À ce sujet, Roy Pfitzner (informaticien au sein du Commissariat à la protection des données du Land de Brandebourg) écrivait déjà en 2003 que les techniques d'informatique de confiance (TCPA) étaient souvent

Fachartikeln, Promotionen und sogar in eine Anfrage der CDU/CSU-Fraktion an den Bundestag gefunden.“ [Pfit03] Hintergrund dieser einseitigen Rezeption einer Technologie ist, dass auch als datenschutzfeindlich betrachtete Zwecke gefördert werden können, insbesondere können Konsumenten digitaler Waren (z. B. Musikstücken) zur Preisgabe personenbezogener Daten gezwungen werden, wenn sie an einem geschlossenen System der Distribution teilnehmen.	assimilées à un système de gestion des droits numériques (DRM) non respectueux de la protection des données personnelles et signalait l’apparition de jugements négatifs sur les techniques d’informatique de confiance (TCPA) dans des articles scientifiques, des thèses et même dans une question du groupe CDU/CSU au Bundestag. [Pfit03] Cette perception quasi unanime s’explique par la possibilité d’utiliser ces technologies à des fins jugées non conformes à la protection des données – principalement parce que les consommateurs de produits numériques (de musique, par ex.) sont obligés de renseigner leurs données personnelles lorsque la transaction a lieu au sein d’un système de distribution fermé.
Fußnote	**Note de bas de page**
[2]Trusted Computing Platform Alliance (TCPA) war ein Konsortium, das 1999 von Microsoft, IBM, und weiteren Herstellern gegründet wurde. Inzwischen wurde es von der von der Nachfolgeorganisation Trusted Computing Group (TCG) abgelöst.	[2] L’Alliance pour une informatique de confiance (TCPA) (en anglais, *Trusted Computing Platform Alliance* − TCPA) est un consortium fondé en 1999 par Microsoft, IBM, et d’autres éditeurs. Il a ensuite été dissout par l’organisation qui lui a succédé, le groupe TCG (Trusted Computing Group).

3 Prototypische Realisierung	**3 Réalisation d'un prototype**
Die Nutzung von PC-Architektur, TPM-Technologie und eines Sicherheitskernels (z. B. emscb/Turaya), der einen sicheren Bootvorgang und die Überprüfung einer sicheren Systemkonfiguration zulässt, ermöglicht bereits eine technologische Realisierung, die im folgenden skizziert wird.	L'utilisation d'une architecture PC, de la technologie TPM et d'un système d'exploitation basé sur un noyau sécurisé (par ex. *emscb/Turaya*), autorisant une procédure de démarrage et un contrôle de configuration de système sécurisés, suffit à mettre en œuvre le dispositif technique présenté ci-dessous.
Der PC-basierte Prototyp bootet (unter Nutzung von *TrustedGRUB*[3] und einem Linuxbasierten Microkernel) in eine als sicher definierte Systemkonfiguration und startet dann die Applikation mit der Datenschutzanwendung. Die zu schützenden Rohdaten sind nur in verschlüsselter Form auf der Festplatte gespeichert; der hier genutzte Schlüssel kann mithilfe des TPM-Chips in der sicheren Konfiguration berechnet werden (er wird vom sog. Storage Root Key abgeleitet). Die Applikation liest die (digital signierte) maschinenlesbare Rechtebeschreibung ein und lässt gemäß des DRM-Konzeptes und vorliegender Rechtebeschreibung entsprechende Zugriffe auf die Datenbasis zu.	Lorsqu'on utilise *TrustedGRUB*[3] et un système d'exploitation basé sur le noyau Linux, le prototype basé sur une architecture PC démarre en définissant une configuration sécurisée et met en route l'application de protection des données. Les données brutes à protéger ne sont enregistrées sur le disque dur que sous forme chiffrée, la clé utilisée dans cet exemple peut être générée à l'aide de la puce TPM sous configuration sécurisée (elle est dérivée de la clé racine de stockage – *Storage Root Key*). L'application déchiffre (à l'aide d'une signature numérique) l'expression des droits codée informatiquement et autorise l'accès adéquat à la base de données en fonction du modèle DRM et de la position effective de l'expression des droits.
Der Beitrag beschreibt drei Anwendungsfälle (Kunden-Datenschutz, Mitarbeiter-Datenschutz und Elektronische Fahndung / Datenabgleich).	Trois domaines d'application pratique sont étudiés dans cet article (*la protection des données des clients, la protection des données des employés* et *l'investigation numérique/le rapprochement de données*).
Fußnote	**Note de bas de page**
[3]Erweiterung des Linux-Bootloaders GRUB. URL: http://www.sirrix.com/content/pages/trustedgrub.htm	[3]Extension du gestionnaire de démarrage Linux basé sur GRUB. URL : http://www.sirrix.com/content/pages/trustedgrub.htm
3.1 Anwendungsbeispiel: Kunden-Datenschutz	**3.1 Domaine d'application pratique : la protection des données clients**
Die Anwendung für den Kunden-Datenschutz sieht eine Erfassung von (Neu-)Kunden am Mitarbeiter-PC oder automatisiert über eine Webapplikation vor. Hier werden kritische personenbezogene Daten gespeichert (Name, Adresse, Kontodaten: Kontonummer und BLZ u. a.). Die Datenbank umfasst auch operationelle Datensätze eines Kunden (z. B. aktive Bestellungen, abgeschlossene Vorgänge). Der funktionale Rahmen, der hier berücksichtigt wird, umfasst die Anforderungen:	La *protection des données clients* est une application qui envisage la saisie de (nouveaux) clients : manuelle, à partir du poste informatique d'un salarié, ou automatique, via une application web. Il s'agit ici d'enregistrer des données personnelles sensibles (noms, adresses, numéros de compte, codes banque, etc.). Les opérations effectuées par le client sont elles aussi enregistrées dans la base de données (par ex. les commandes en cours, les dossiers archivés). L'environnement fonctionnel considéré ici prend en charge les contraintes suivantes :
• Auskunftsersuchen (Kunden wollen ihre personenbezogenen Daten abfragen)	• demandes d'accès à l'information (les clients souhaitent consulter leurs données personnelles) ;
• Versenden (Adressausgabe) bei Vorliegen eines Auftrages	• envois (à l'adresse renseignée) en cas de formulation de requêtes ;

• Sichere Löschung (nach Ablauf der Aufbewahrungsfrist)	• effacement sécurisé (après expiration du délai de conservation) ;
• Marketingkampagnen (Bedrucken von Briefumschlägen mit Kundenadressen	• campagnes de marketing (impression d'enveloppes à l'adresse des clients) ;
• Weitergabe eines Datensatzes an dritte Partei nach Zustimmung des Kunden	• transfert d'un enregistrement de données à un tiers sous réserve du consentement préalable du client ;
• Backup-Funktionalität	• fonction de sauvegarde.
Die Plattform (siehe Abbildung 1) stellt dabei zuverlässig technisch sicher, dass bestimmte Funktionalitäten ausgeschlossen werden, insbesondere sind dies:	La plateforme technique sécurisée garantit le rejet de certaines fonctionnalités (voir figure 1). Les principales sont :
• Kopieren oder Ausdrucken des Datenbestandes • „Stöbern" im Datenbestand ohne das Hinterlassen von Protokollspuren • Wiederherstellen irreversibel verschlossener oder gelöschter Daten (z. B. nach Diebstahl oder Beschlagnahme, auch nicht für den Datenbankbesitzer) • Weitergabe ohne Zustimmung (sofern dies aus dem Bestand geschieht)[4] • Gleichzeitiges Verändern mehrerer Datensätzen ohne nachgewiesenes Privileg	• la copie et l'impression de l'ensemble des données enregistrées ; • la « fouille des données » sans traces d'exécution ; • la restauration de données définitivement chiffrées ou de données effacées (par ex. suite au vol ou à la captation des données, y compris pour le propriétaire de la base de données) ; • le transfert non autorisé du fichier (s'il est extérieur à la base de données)[4] ; • une modification simultanée de plusieurs enregistrements de données sans privilèges d'authentification.
Fußnote	**Note de bas de page**
[4]Die Plattform kann nicht verhindern, dass bereits bei der Datenerfassung eine Weitergabe erfolgt.	[4] La plateforme ne peut pas empêcher qu'un transfert se produise dès la collecte.

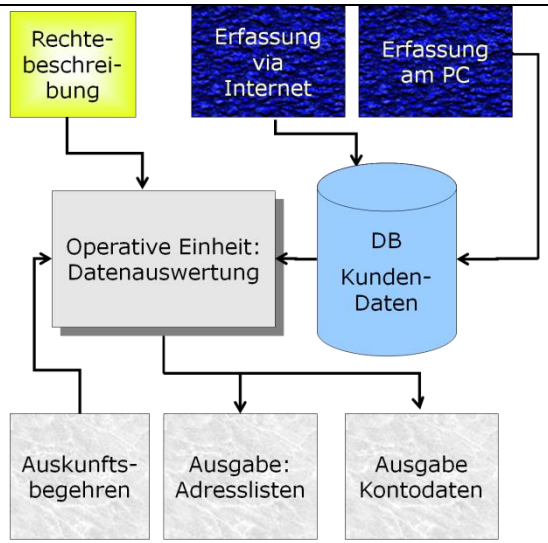


Abbildung 1 Anwendung: Kundendatenschutz

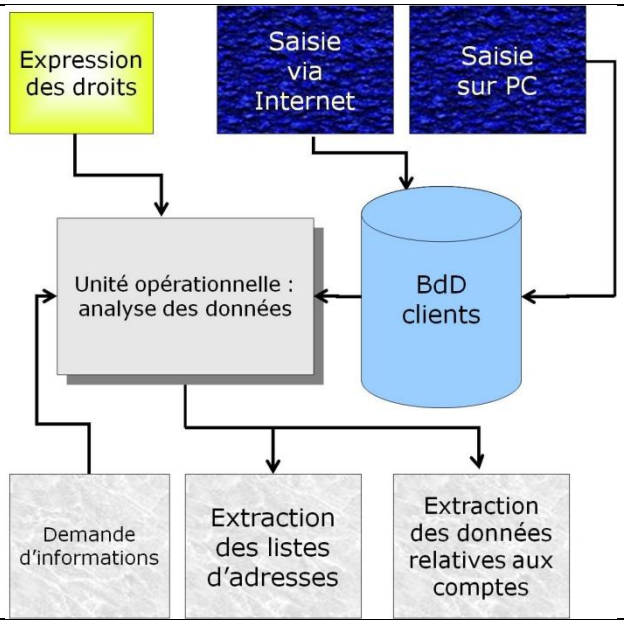


Figure 1 Application à la protection des données clients

3.2 Anwendung: Mitarbeiter-Datenschutz	**3.2 Domaine d'application pratique : protéger les données des employés**
Die Anwendung für den Mitarbeiter-Datenschutz sieht eine Datenhaltung für Arbeitszeitdaten vor, d. h. es werden Daten gewonnen, die über Arbeitszeiterfassungsgeräte erfasst werden. Diese Geräte können beispielsweise in der Nähe von Zugangstüren angebracht sein, oder es handelt sich um mobile Geräte, mit denen Mitarbeiter den Beginn oder das Ende eines Arbeitseinsatzes oder einer Schicht erfassen.	L'application à la *protection des données des employés* concerne la conservation des données de temps de présence, ce qui suppose que les données collectées seront acquises au moyen d'un dispositif de contrôle du temps de présence. Ces appareils, utilisés par les employés pour saisir le début ou la fin d'une activité ou d'un poste, sont, par exemple, installés à proximité des portes d'accès, ou se présentent comme des dispositifs mobiles.
Es wird folgende Funktionalität benötigt	Les fonctionnalités suivantes sont requises :
• Arbeitszeitbeginn und -ende (Arbeitszeitdaten) werden gespeichert Für jeden Mitarbeiter wird ein Stundenkonto geführt • Es werden statistische Daten über Arbeitszeiten ausgegeben • Eine Backup-Lösung (bzw. Tagesaktuelles Cloning einer Datenbank) wird integriert	• enregistrement de l'heure de début et de fin du poste de travail ; • ouverture d'un compte horaire pour chaque salarié ; • génération de statistiques sur les temps de présence ; • intégration d'une solution de sauvegarde (ou de réplication journalière de la base de données).

Die Komponenten und ihre Beziehungen untereinander werden in der Abbildung 2 vereinfacht dargestellt.	La figure 2 est une représentation simplifiée des différents composants et de leurs interactions.

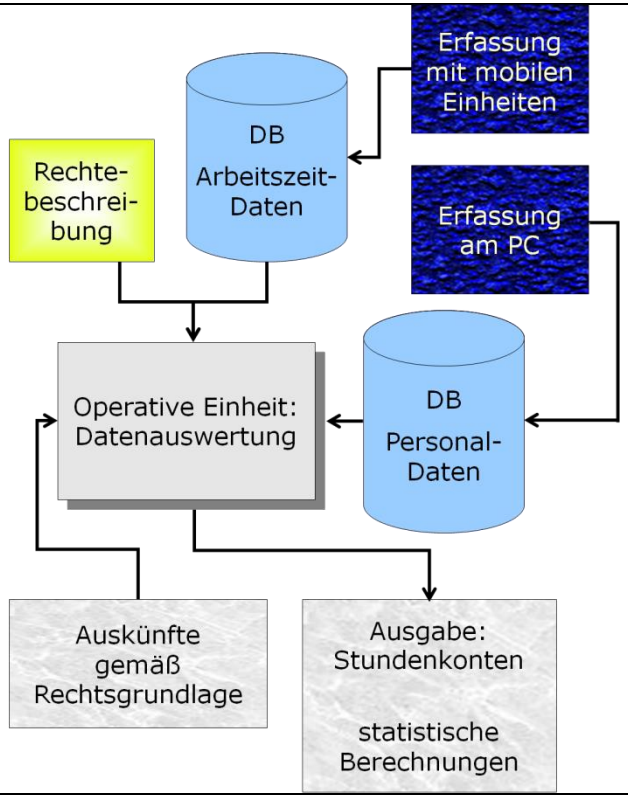
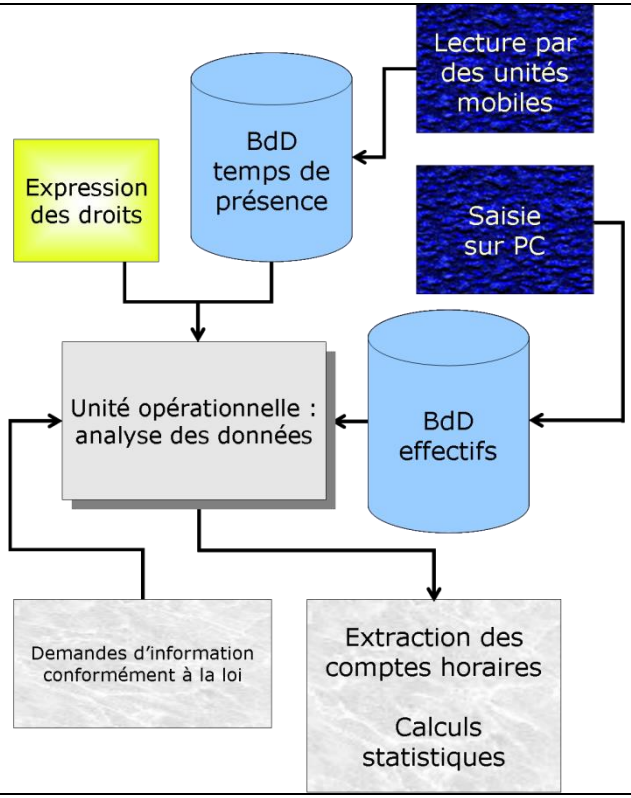

	

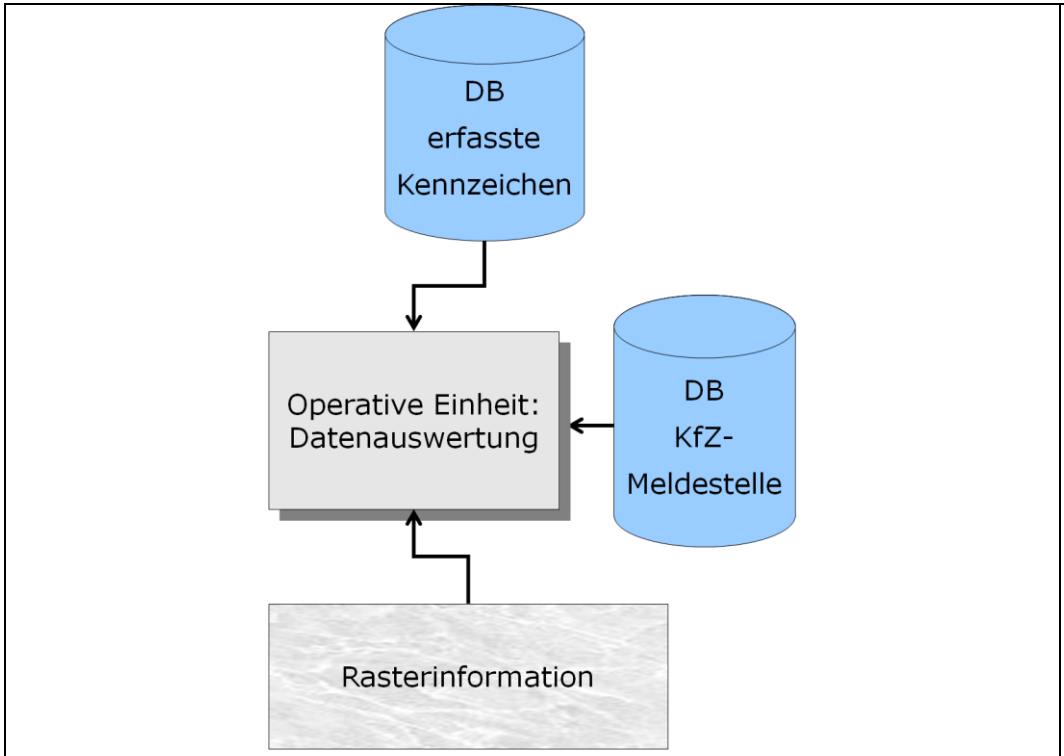
Abbildung 2 Anwendung für den Mitarbeiter-Datenschutz	*Figure 2 Application à la protection des données des employés*
Die Operative Einheit muss hierbei nicht notwendigerweise eine eigenständige Komponente sein, die eine sichere Kommunikationsbeziehung zu den beiden Datenbanken aufbaut, sie kann durchaus in eine (oder beide) Datenbank-Komponenten integriert sein.	Dans ce cas de figure, l'unité opérationnelle peut très bien être intégrée à l'un des composants de la base de données (ou aux deux). Elle n'est pas obligatoirement un composant autonome qui unit les deux bases de données via un lien de communication sécurisé.

Die Anforderungen an die Komponente DB Arbeitszeitdaten sind hierbei:	Les composants de la *BdD temps de présence* sont paramétrés comme suit :
• Die Arbeitszeitdaten können nicht exportiert werden (von den nun folgenden Ausnahmen abgesehen). • Die Arbeitszeitdaten sind nach Ablauf der Aufbewahrungsfrist zu löschen • Die Stundenkontenstände der Mitarbeiter werden regelmäßig (z. B. wöchentlich) ausgegeben (Export im Klartext z. B. an ein SAP-System). • Arbeitszeitdaten eines einzelnen Mitarbeiters können über eine bestimmte Rolle angefordert und ausgegeben werden. Erlaubte Suchparameter sind durch eine maschinenlesbare Rechtebeschreibung definiert.	• impossibilité d'exporter les données de temps de présence (sauf exceptions ci-dessous) ; • obligation d'effacer les données de temps de présence après expiration de leur délai de conservation ; • émissions régulières (par ex. une fois par semaine) de rapports sur la situation des comptes horaires des employés (exportation de données en clair, par ex. dans un système SAP) ; • demandes de consultation et extraction des données de temps de présence d'un salarié individuel pour un poste spécifique. Les paramètres de recherche autorisés sont définis par une *expression de droit* lisible par machine.
Der datenschutzrechtliche Rahmen, der hier funktional abgebildet werden soll, besteht in folgenden Anforderungen.	Les paramètres ci-dessous constituent le cadre juridique de la protection des données. Cet exemple cherche à reproduire son fonctionnement :
• Arbeitszeitdaten sind personenbezogene Daten, die ausschließlich zu festgelegten Zwecken (Stundenkonto) verarbeitet werden • Ein Mitarbeiter kann Auskunft über gespeicherte Daten zu seiner Person verlangen (z. B. um Abrechnungsvorgänge nachzuvollziehen) • In begründeten Fällen (und mit Zustimmung der Personalvertretung) können einzelne Mitarbeiter aufgrund ihrer Arbeitszeitdaten identifiziert werden (z. B. um eine Straftat aufzuklären). Anfragen dieser Art können nur von einer bestimmten Rolle und in einem gewissen Rahmen zugelassen werden.	• les données de temps de présence sont des données personnelles, qui seront utilisées uniquement dans un but précis et déterminé (compte horaire) ; • un salarié peut demander l'accès aux données enregistrées qui le concernent (par ex. pour suivre les procédures de calcul) ; • dans les cas légitimes (et avec l'accord des représentants du personnel), les données des temps de présence peuvent justifier une recherche sur l'identité d'employés (par exemple, pour clarifier une situation conflictuelle). Ce type de demandes ne peut être autorisé que par un type d'utilisateur précis et dans un cadre spécifique.
Der letztgenannte Punkt sieht eine Zusammenführung von Daten beider Datenbanken (DB Personaldaten und DB Arbeitszeitdaten) vor und erfordert eine detaillierte Feinspezifikation, da hier zunächst zu untersuchen ist, inwieweit der rechtliche Rahmen überhaupt mittels einer technischen Rechtebeschreibung kodierbar ist. Die Komponente kann wirksam gewisse Klassen von unzulässigen Anfragen verhindern (z. B. solche Anfragen, deren Ergebnis eine Ausgabe der Arbeitszeitdaten von zu vielen Mitarbeitern zur Folge hätte).	Ce dernier aspect suppose un rapprochement des informations des deux bases de données (*BdD effectifs* et *BdD temps de présence)* et requiert une spécification fine et détaillée. En effet, il s'agit avant tout, dans cet exemple, d'évaluer dans quelle mesure le cadre juridique peut être retranscrit sous forme de code informatique dans un langage d'expression des droits. Le composant (TPM) peut bloquer efficacement certaines catégories de requêtes (par ex., des requêtes dont le résultat entraînerait la divulgation des données de temps de présence d'un trop grand nombre d'employés).

Statistische Berechnungen sollen zudem möglich sein, sofern keine Gewinnung der Rohdaten (hier: Arbeitszeitdaten) möglich ist. Für die Betriebsleitung kann es beispielsweise interessant (und legitim) sein, zu erfahren, wie viele Mitarbeiter vor einem bestimmen Zeitpunkt mit den Dienstgeschäften beginnen (Parkraumbewirtschaftung), zu welcher Zeit die Mittagspause genommen wird (Kantinenorganisation) oder wie viele Personen sich in einem Gebäude aufhalten (Sicherheitsüberlegungen). Die Rechtebeschreibungssprache muss dabei mächtig genug sein, sowohl die Art der statistischen Berechnung abzubilden (z. B. vollständige SQLStatements integrieren) als auch Beschränkungen parametrisierbarer Anforderungen zu überwachen, die zur De-Anonymisierung genutzt werden könnten (Parameterkombinationen müssen beschränkt werden können).	De plus, la génération de statistiques n'est autorisée que dans la mesure où l'acquisition des données brutes est impossible (en l'occurrence : les données de temps de présence). Pour la direction, il peut être, par exemple, intéressant (et utile) de savoir combien d'employés effectuent leur prise de service avant une certaine heure (occupation du parking), à quelle heure ils prennent leur pause déjeuner (organisation du restaurant d'entreprise) ou combien de personnes se trouvent à l'intérieur d'un bâtiment (considérations de sécurité). Le langage d'expression des droits doit être suffisamment puissant pour pouvoir élaborer des modèles statistiques (par ex., intégrer des requêtes SQL complètes) comme pour pouvoir contrôler les limitations assignées aux paramètres configurables. En effet, ces derniers pourraient être utilisés pour désanonymiser les données (il doit être possible de limiter les combinaisons de paramètres).
Der Aspekt Auskunftsrecht ist für die Architektur problematisch, da ein irreversibler Verschluss nicht mehr gegeben ist, wenn eine privilegierte Rolle einzelne Rohdatensätze anfordern kann (diese Rolle könnte dann alle Datensätze auslesen). Hier ist unter Abwägung des rechtlichen Rahmens und der Wirksamkeit des Schutzes zu entscheiden, ob diese Schwachstelle akzeptiert wird oder ob das Auskunftsrecht ebenfalls insoweit beschränkt wird, dass nach Erreichen eines Schwellenwertes keine Auskünfte möglich sind. Die Daten könnten dann nur noch in Gänze gelöscht werden, um Einzelinteressen zu befriedigen.	Le *droit d'accès* pose problème pour l'architecture. En effet, il n'y a plus de *chiffrement à sens unique*, dès lors qu'un statut privilégié peut demander l'accès aux enregistrements de données brutes (le détenteur de ce statut pourrait ensuite sélectionner tous les enregistrements de données). Une fois que le cadre juridique a été comparé à l'efficacité de la protection, il faut décider d'accepter cette faille ou de limiter aussi le droit d'accès, pour rendre toute demande impossible dès lors qu'une valeur seuil est atteinte. Seul l'ensemble des données pourra ensuite être effacé au service des intérêts individuels.
3.3 Anwendung: Elektronische Fahndung / Datenabgleich	**3.3 Domaine d'application : investigation numérique/rapprochements de données**
Bei einer Rasterfahndung werden personenbezogene und personenbeziehbare Daten anhand eines vorgegebenen Rasters (Profil eines Täters) aus verschiedenen meist sehr umfangreichen Datenbeständen zusammengeführt. Ziel ist die Ermittlung des Täters bzw. die Gewinnung einer überschaubaren Menge verdächtiger Personen, die weiter überprüft werden kann. Im hier dargestellten Beispiel (siehe Abbildung 3) liegt eine Beschreibung eines verdächtigen Fahrzeugs als Rasterinformation vor (Marke, Typ, Farbe) und eine Datenbank mit erfassten Kennzeichen[5] über einen definierten Zeitraum; die Fahndung kann hier elektronisch durchgeführt werden. Im Jahre 2006 erfolgte ein wegweisender Beschluss des Bundesverfassungsgerichtes zur Definition und zur Zulässigkeit einer solchen Fahndungsmaßnahme.	L'analyse sérielle[5] est une méthode d'investigation qui consiste à rapprocher des données personnelles et des renseignements sur les personnes à partir de plusieurs bases de données, en général très importantes, à l'aide d'une matrice donnée (le profil du suspect). Elle a pour objectif d'identifier le suspect ou de dégager un nombre raisonnable d'individus suspects qui feront ensuite l'objet d'une enquête. Dans cet exemple (voir figure 3), on dispose de la description d'un véhicule suspect (marque, modèle, couleur) et d'une base de données contenant des numéros d'immatriculation relevés[6] au cours d'une période déterminée ; on peut donc procéder ici à une investigation numérique. En 2006, la Cour constitutionnelle allemande a rendu une décision historique sur la définition et la recevabilité de ce type de mesures d'investigation.

Fußnote	**Notes de bas de page**
	[5] En allemand *Rasterfahndung*, N.d.T. [6] D'après la décision de la Cour constitutionnelle allemande de mars 2008 (n° 1 BvR 2074/05 et 1 BvR 1254/07), la reconnaissance automatique des immatriculations, autorisée par les lois des Länder de Hesse et du Schleswig-Holstein, est anticonstitutionnelle. Dans son commentaire oral de la décision, le président de la Cour, Hans-Jürgen Papier, considère que l'atteinte au droit fondamental est mineure lorsque les immatriculations reconnues servent uniquement à identifier des véhicules volés ou bien des escroqueries à l'assurance et que tous les résultats qui ne correspondent pas à la recherche sont immédiatement effacés, sans conserver aucune trace. Mais plus l'atteinte est grave (par ex. en cas d'enregistrement des données), plus le cadre juridique autorisant la police à agir doit être clair et précis. Plusieurs Länder préparent en ce moment de nouvelles réglementations juridiques.

Beschluss des BVG vom 4. April 2006 – 1 BvR 518/02 (Auszug):	**Décision de la Cour constitutionnelle allemande du 4 avril 2006 – 1 BvR 518/02 (extrait)[7] :**
Die Rasterfahndung ist eine besondere polizeiliche Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Polizeibehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich mit anderen Daten vorzunehmen. Durch den Abgleich soll diejenige Schnittmenge von Personen ermittelt werden, auf welche bestimmte, vorab festgelegte und für die weiteren Ermittlungen als bedeutsam angesehene Merkmale zutreffen. (...)	**L'analyse sérielle est une méthode spécifique d'investigation policière qui utilise le traitement électronique des données. Les autorités de police demandent à d'autres organisations publiques ou privées de leur transmettre des données personnelles, afin de procéder à un rapprochement automatique avec d'autres données. Ce rapprochement doit permettre d'identifier les personnes dont les caractéristiques correspondent à des critères définis au préalable et considérés comme des éléments déterminants pour la suite de l'enquête. […]**
Angesichts des Gewichts der mit der Durchführung einer Rasterfahndung einhergehenden Grundrechtseingriffe ist diese nur dann angemessen, wenn der Gesetzgeber rechtsstaatliche Anforderungen dadurch wahrt, dass er den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für die bedrohten Rechtsgüter an vorsieht.	**Considérant que la mise en œuvre d'une investigation par recoupement constitue une grave atteinte au droit fondamental, elle n'est proportionnée que lorsque le législateur, s'appuyant sur les principes du droit, considère qu'un danger concret et imminent représente une menace supérieure pour les biens juridiques.**
Eine Vornahme der Rasterfahndung kann in technischer Hinsicht darin bestehen, alle erfassten Kennzeichen eines definierten Zeitraums (gemäß Tatzeitpunkt) zu ermitteln und zu diesen mithilfe der Datenbank der KfZ-Meldestelle eine Tabelle zu bilden, die zeilenweise Einträge über das Kennzeichen, den Halter (Name und Meldeadresse) und das Fahrzeug (Marke, Typ, Farbe) enthält. Unter Verwendung der Rasterinformation kann dann eine Menge von Personen (Fahrzeughaltern) bestimmt werden, die gemäß Rasterinformation als Verdächtige in Frage kommen.	Techniquement parlant, une procédure d'analyse sérielle consiste, par exemple, à enquêter sur tous les relevés de numéros d'immatriculation concernant une période donnée (en fonction de l'heure du délit). Ces numéros ainsi que les informations fournies par la base de données et le fichier des immatriculations de la préfecture permettent de constituer un tableau contenant, ligne par ligne, des informations sur l'immatriculation, le propriétaire (nom et adresse déclarée) et le véhicule (marque, modèle, couleur). Le groupe de personnes considérées comme suspectes est identifié au moyen de cette matrice (parmi les propriétaires de véhicules).
Eine derart vorgenommene Fahndung kann rechtlich zulässig sein, wenn die Angemessenheit gewahrt ist (d. h. es wurden schwerwiegende Straftaten begangen bzw. es besteht weiterhin eine erhebliche Bedrohung). Wenn die Datenbankinhalte den Ermittlern aufgrund eines Beschlusses zur Verfügung gestellt werden (z. B. als exportierter Dump), lässt sich jedoch i. a. nicht mehr nachverfolgen, ob diese nur zu dem benannten Fahndungsvorhaben eingesetzt wurden und ob die Daten nach der Auswertung gelöscht werden.	La conduite de ce type d'investigation peut être autorisée si le principe de proportionnalité est établi (c'est-à-dire que des actes répréhensibles graves ont été commis ou qu'une menace importante existe). Lorsque les contenus des bases de données sont livrés aux enquêteurs à la suite d'une décision de justice (par ex. sous forme de fichiers d'exportation – *dump*), on ne peut en général plus savoir si ils ont été utilisés uniquement dans le cadre des mesures d'investigations précitées et si les données ont été effacées après leur exploitation.
Fußnote	**Note de bas de page**
	[7] Traduction librement adaptée de l'original, N.d.T.



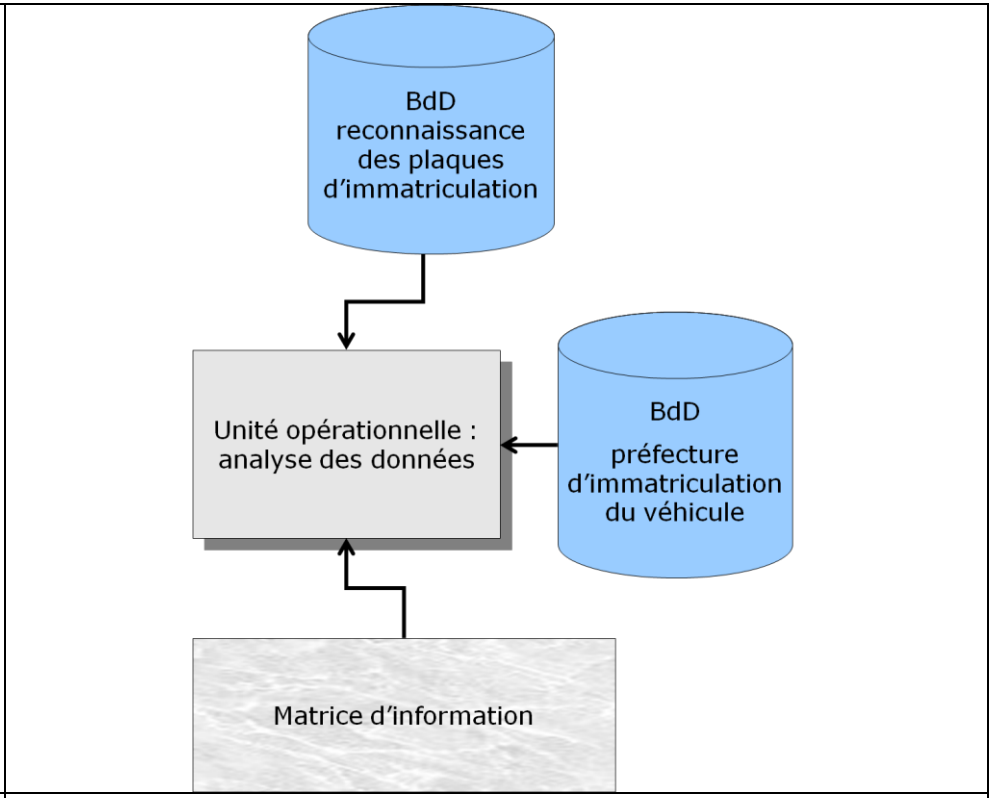


Abbildung 3 Fahndung gemäß eines KfZ-Profils	*Figure 3 Investigation à partir du signalement de la préfecture*
Anforderungen sind hier, dass die Operative Einheit	Dans cet exemple, l'unité opérationnelle est paramétrée pour :
• die Rohdaten erfasst, ohne dass diese Daten dem Ermittler zugänglich sind, • nur eine einmalige Auswertung gemäß des Beschlusses vornimmt, • nur dann die „Treffer" ausgibt, wenn die Gesamtzahl einen im Beschluss festgelegten Schwellenwert nicht überschreitet, • einen signierten Bericht generiert, der die vorgenommenen Operationen dokumentiert und an eine Kontrollinstanz weiterzugeben ist • und die Daten zu einem definierten Zeitpunkt bzw. nach der Auswertung löscht.	• collecter les données brutes sans donner accès à l'enquêteur ; • procéder à une seule et unique utilisation des données conformément à la décision ; • afficher ensuite uniquement les résultats correspondant à cette recherche, à condition de ne pas dépasser la valeur seuil fixée par la décision ; • générer un rapport crypté listant les opérations effectuées et le remettre à une autorité de contrôle ; • et enfin, effacer les données conformément au délai fixé ou directement après leur utilisation.

Es sind weitere Eigenschaften denkbar, die gemäß rechtlicher Grundlagen in die Funktionalität eingebracht werden können (z. B. Verwaltung von Privilegien, Einlesen eines Beschlusses in maschinenlesbarer Form, automatisierte Information der betroffenen Personen zu einem späteren Zeitpunkt, Auskunftsrecht).	D'autres spécifications conformes au cadre juridique et intégrables aux fonctionnalités peuvent être envisagées (par ex. la gestion de privilèges, l'enregistrement d'une décision sous une forme lisible par une machine, l'envoi d'une notification automatique à la personne concernée *a posteriori*, le droit d'accès).
Eine Besonderheit bei diesem Anwendungsfall ist neben den ausgeprägten rechtlichen Beschränkungen die mobile Natur der Datenerfassung. Geräte, die Kfz-Kennzeichen erfassen, werden nur vorübergehend an „Kontrollpunkten" aufgestellt (es existieren jedoch auch stationäre Einheiten).	La mobilité de la collecte des données est une des particularités cette application, au-delà de son cadre juridique très restrictif. Les machines utilisées pour enregistrer les numéros des plaques d'immatriculation ne sont que temporairement installées à des « points de contrôle » (mais il existe aussi des unités fixes).
Wir gehen davon aus, dass nach Erfassung ein Transport eines Datenträgers erfolgt, der eine Liste erfasster Kennzeichen enthält. Um einen Missbrauch der Daten (z. B. durch Duplizierung) frühzeitig zu verhindern, kann hier in der Spezifikation eine Speicherung auf einer Chipkarte vorgesehen werden. Das Kennzeichenlesegerät überträgt die Daten unmittelbar an eine eingesteckte Chipkarte, die sowohl als (mobiler) Datenträger fungiert als auch bereits das „Datengrab" (irreversibler Verschluss) darstellt, d. h. die gelesenen Daten werden die Karte nicht mehr verlassen (die Chipkarte enthält also die DB Erfasste Kennzeichen im EEPROM).	Nous partons du principe qu'une fois collectées, les données sont transférées sur un support qui contient la liste des numéros d'immatriculation qui ont été déclarés. Pour empêcher, le plus tôt possible, l'utilisation des données dans un but frauduleux (par ex. leur duplication), les spécifications peuvent, dans ce cas, prévoir un enregistrement sur une carte à puce, qui servira à la fois de support de données (mobile) et de « cimetière de données » (chiffrement à sens unique), ce qui veut dire que les données enregistrées ne disparaîtront jamais de la carte (la carte à puce contient donc la base de données *BdD numéros d'immatriculation collectés* en EEPROM).
Die Operative Einheit ist demnach in der Lage, sich gegenüber der Karte zu authentisieren und eine Suche auf den Daten vorzunehmen bzw. die Daten unter DRM-Beschränkung zu importieren.	L'unité opérationnelle est dès lors capable de s'authentifier auprès de la carte et d'entreprendre une recherche de données ou d'importer les données en obéissant aux limitations DRM.
3.4 Sicherheitsbetrachtungen und politische Brisanz	**3.4. Considérations de sécurité et controverses autour du sujet**
Die Durchsetzung der digitalen Rechte zu Datenschutzzwecken stützt sich auf die Fähigkeit der vertrauenswürdigen Hardware, den Zugriff auf unverschlüsselte Daten tatsächlich allein auf sichere Konfigurationen zu beschränken. Angriffe auf Hardware-basierte Sicherheitsfunktionalität auf Grundlage des TPM zeigen [Gree07, Kaue07, KSP05], dass Schwachstellen für (zu dieser Zeit verfügbare) TPM-basierte Plattformen existieren, die unter günstigen Umständen zur Kompromittierung der Plattform ausgenutzt werden können. Eine prototypische Realisierung muss daher den aktuellen Stand der Verwundbarkeit Hardware-basierter Sicherheit berücksichtigen, wenn eine Aussage zur Mechanismenstärke bzw. zum erzielten Sicherheitslevel getroffen wird.	L'adoption de systèmes de gestion des droits numériques repose sur la capacité du matériel de confiance à restreindre seul l'accès aux données non cryptées en utilisant uniquement des configurations sécurisées. Des attaques sur des fonctions de sécurité basées sur du matériel informatique intégrant un module TPM démontrent que les plateformes (disponibles à l'heure actuelle) présentent des failles qui, lorsque les circonstances s'y prêtent, peuvent être utilisées pour corrompre la plateforme. C'est pourquoi l'état actuel des vulnérabilités liées à la sécurité du matériel informatique doit être pris en compte dans la réalisation du prototype, au moment de définir les assertions définissant la robustesse du mécanisme ou le niveau de sécurité escompté.

Eine Speicherung der Datenbestände allein bei einem öffentlich bestelltem Datenspeicherer bei gleichzeitiger Durchsetzung eines weitreichendem Verbots der sonstigen Speicherung personenbezogener Daten und erheblicher Lockerung der Anforderungen an eine Speicherung personenbezogener Daten stellt eine erhebliche Änderung der datenschutzrechtlichen Bestimmungen dar, so dass ein solche Neuregelung eine revolutionäre Anpassung des Datenschutzrechts bedeuten würde. Dieses Änderung wurde für den Vortrag (gehalten anlässlich der MinD-Akademie 2009 in Nürnberg) im Rahmen eines Gedankenexperiments detailreich ausgemalt: Könnten sich die Zuhörer individuell vorstellen, dass alle anfallenden Daten (Lokalisierung der Person, Suchmaschinenabfragen, Telekommunikationvorgänge, Kontobewegungen) über sie gespeichert werden, wenn die Speicherung für einen „guten Zweck“ (z. B. Fahndungszwecke) erfolgt, wenn sie bei Verarbeitung der Daten zwingend informiert werden (Konfiguration der automatischen Benachrichtigung vorausgesetzt) und wenn die Speicherung nicht mehr bei der erhebenden Partei erfolgt?	Une autorité d’enregistrement certifiée, seule autorisée à enregistrer l’ensemble des données, assortie d’une interdiction large d’enregistrer toute autre donnée personnelle et d’un chiffrement strict des paramètres d’enregistrement, représente un changement majeur au regard des dispositions du droit à la protection des données. L’adaptation du droit à la protection des données à cette nouvelle règle serait une révolution. Ce changement a été décrit de manière détaillée à l’occasion de la conférence MinD en 2009 à Nuremberg. Nous avons alors demandé au public présent dans la salle s’il était favorable à l’enregistrement de toutes les données accumulées (localisation physique, requêtes de moteurs de recherche, données de télécommunications, mouvements de comptes bancaires), dès lors : • que la finalité de l’enregistrement est « légitime » (par ex. à des fins d’investigation) ; • qu’il est obligatoirement informé du traitement dont ses données font l’objet (ce qui suppose la configuration d’une notification automatique) ; • et que l’enregistrement n’est plus réalisé par le tiers collecteur.
Das Ergebnis war vielschichtig: Einer solchen erhebliche Änderung der rechtlichen Bestimmungen würde fast niemand ohne genaueste Prüfung der rechtlich-politischen Konsequenzen zustimmen; die zwingende Benachrichtigung der Personen bei Verarbeitung von auf sie bezogenen Daten (dies beträfe dann auch beispielsweise die Google-Suche nach einem seltenen Vor- und Nachnamen) wurde überwiegend positiv aufgenommen; die gesamte Speicherung aller anfallenden Daten jedoch überwiegend als „unnötig gefährlich“ betrachtet (Repräsentativität wird vom Autor nicht angenommen, da es eine offene Diskussion in großer Runde war). Die grundsätzliche Skepsis gegenüber der technischen Fähigkeit, die Daten auch bei einem unabhängigen Datenspeicherer vor Missbrauch zu schützen, war deutlich spürbar. Gleichzeitig wirkte das Gedankenexperiment auf einige Teilnehmer in Bezug auf das Thema Datenschutz sensibilisierend, da es nicht allen bewusst war, welche Daten bereits zum Zeitpunkt des Vortrages aufgrund der gesetzlichen Vorgabe der sog. Vorratsdatenspeicherung bei Telekommunikationsunternehmen gespeichert werden oder bei Suchmaschinenbetreibern anfallen und mit zweifelhaftes rechtlicher Grundlage ebenfalls gespeichert werden. Die Praxis der Vorratsdatenspeicherung wurde zwischenzeitlich nach einem Urteil des Bundesverfassungsgerichtes vom 02.03.2010 bis zu einer gesetzlichen Neuregelung beendet.	Les réactions ont été contrastées : presque aucune des personnes présentes dans le public n’était prête à accepter un tel changement des dispositions juridiques actuelles sans un examen complet de ses conséquences politico-juridiques ; une majorité d’entre elles accueille favorablement l’obligation d’informer la personne concernée lorsque ses données font l’objet d’un traitement (cela pourrait ensuite concerner les recherches sur les noms et les prénoms avec *Google*) ; enfin, l’enregistrement systématique de toutes les données accumulées est majoritairement perçu comme un « risque inutile » (s’agissant d’une discussion avec la salle, l’auteur ne suppose pas que les résultats sont représentatifs). La capacité de la technique à protéger les données, même confiées à une autorité d’enregistrement indépendante, contre les utilisations frauduleuses, a suscité de sérieux doutes. Par ailleurs, cette expérience de pensée a eu un effet de sensibilisation au thème de la protection des données sur quelques-uns des participants. En effet, au moment de la présentation, tous ne savaient pas exactement quelles données étaient déjà susceptibles d’être enregistrées en vertu des obligations légales relatives à la conservation des données de connexion enregistrées par les opérateurs de télécommunications ou accumulées par les fournisseurs de moteurs de recherche, puis enregistrées de la même façon, en jouant sur l’ambiguïté du droit. Depuis, le jugement de la Cour

	constitutionnelle allemande du 2 mars 2010 a suspendu la pratique de la conservation des données de connexion jusqu'à l'adoption d'une nouvelle réglementation juridique.
Aus wissenschaftlicher Sicht sind abgesehen von der potentiellen Verwundbarkeit der Hardware- Plattform konzeptionelle Fehler bei der Rechtebeschreibung bzw. dem Parsing der maschinenlesbaren Rechte zu berücksichtigen. Eine Realisierung für produktive Anwendungen sollte daher einer Evaluation gemäß etablierter Sicherheitskriterien (z. B. Common Criteria) unterzogen werden, um eine unabhängige Prüfung der Rechtebeschreibung und der technischen Durchsetzung zu gewährleisten.	Du point de vue scientifique, hormis l'éventuelle vulnérabilité de la plateforme matérielle, il convient de prendre en compte les failles dans la conception de l'expression des droits ou de l'analyse syntaxique (*parsing*) des droits lisibles par une machine. La mise en service d'applications productives doit s'appuyer sur une évaluation de conformité à des critères de sécurité reconnus (par ex. *Common Criteria*), pour garantir l'indépendance de l'examen de l'expression des droits et de la conception technique.
4 Fazit und Ausblick	**4 Résumé et conclusion**
Das Konzept des „irreversiblen Verschlusses" erweitert das Prinzip der „Datensparsamkeit und Datenvermeidung" durch Einführung eines technischen Werkzeuges. Unter Nutzung vertrauenswürdiger Hardware und technologischer Ansätze der Digitalen Rechteverwaltung kann eine Technologie realisiert werden, die Daten speichert und für einen definierten Zweck verarbeitet, eine Weitergabe jedoch wirksam verhindert.	La notion de « chiffrement à sens unique » prolonge le principe de limitation de la collecte par l'introduction d'un dispositif technique. En utilisant du matériel de confiance et une approche technologique basée sur la gestion des droits numériques, on peut mettre en place un système capable d'enregistrer les données et de procéder à leur traitement pour une finalité déterminée, tout en bloquant efficacement les transferts de fichiers.
Eine Erweiterung des Datenschutzrechts auf Grundlage der Technologie, die eine Verbreiterung der ~~der~~ Speicherung unterworfenen anfallenden Datenbasis bei zwingender Information des Betroffenen bei Verarbeitung der personenbezogenen Daten vorsieht, könnte ein Weg sein, Sicherheitsinteressen des Staates bei gleichzeitiger Erhöhung der Transparenz der personenbezogener Datenverarbeitung vorzusehen. Der üblicherweise angenommene Trade-Off (weniger Datenschutz → mehr Sicherheit) würde bei diesem Konzept für Teilbereiche aufgehoben. Die Vermittlung der technologischen Grundlagen gegenüber breiter Bevölkerungsschichten und politisch Handelnder wäre jedoch eine Voraussetzung, damit die politische Durchsetzbarkeit und rechtlich zulässige Umsetzung gegeben ist. Derzeit gibt es jedoch noch keine Anzeichen dafür, dass ein tiefes informationstechnisches Wissen über den harten Kern der Internet-Community hinaus in breiten Schichten vorhanden ist; hier wäre es wohl auch die Bringschuld der technischen Experten, Konzepte und Technologien des technisches Datenschutzes „massentauglich" zu vermitteln.	Une modernisation du droit à la protection des données, fondée sur une technologie dont le principe consiste à étendre les enregistrements aux données acquises et accumulées, et en contrepartie à informer systématiquement la personne concernée lorsque ses données personnelles sont utilisées, serait un moyen de concilier les intérêts sécuritaires de l'État et une meilleure transparence du traitement des données relatives à la personne. Cette idée permet en partie de dépasser le clivage traditionnel : moins de protection des données, plus de sécurité. Pour autant, les mesures visant à imposer ces principes techniques et à les transposer en droit ne verront le jour que si un public plus large au sein de la population et parmi les acteurs politiques est sensibilisé. Or, le noyau dur de la communauté internet ne semble pour le moment pas encore être parvenu à diffuser une meilleure connaissance des techniques informatiques auprès d'un public plus large ; dans ce domaine, les spécialistes de l'informatique ont aussi un rôle à jouer : celui d'aider le plus grand nombre à comprendre les notions et les technologies relatives à la protection des données.

Literatur und Quellen	Documents et sources
[Afp08] Meldung der Agentur AFP vom 04.10.2008	[Afp08] Communiqué de l'agence France-Presse, 04.10.2008.
[Netz07] Bericht der Netzeitung, http://www.netzeitung.de/ausland/848950.html.	[Netz07] Reportage de Netzeitung, http://www.netzeitung.de/ausland/848950.html.
[Bech05] Stefan Bechtold: Trusted Computing: *Rechtliche Probleme einer entstehenden Technologie*. Oktober 2005.	[Bech05] Stefan Bechtold : Trusted Computing: *Rechtliche Probleme einer entstehenden Technologie*. Octobre 2005.
[BöPf08] Rainer Böhme, Andreas Pfitzmann: *Digital Rights Management zum Schutz personenbezogener Daten?* DuD (Datenschutz und Datensicherheit), Heft 5/2008.	[BöPf08] Rainer Böhme, Andreas Pfitzmann : *Digital Rights Management zum Schutz personenbezogener Daten?* DuD (Datenschutz und Datensicherheit), n° 5/2008.
[Davi07] Zitiert nach heise online: Monika Ermert: *Persönliches DRM als Retter von Datenschutz und Privatsphäre*. Meldung 99163 vom 18.11.2007. URL: http://www.heise.de/newsticker/meldung/99163 (Stand: Okt. 2008)	[Davi07] D'après une citation de heise online : Monika Ermert : *Persönliches DRM als Retter von Datenschutz und Privatsphäre*. Communiqué 99163, 18.11.2007. URL : http://www.heise.de/newsticker/meldung/99163 (mise en ligne : octobre 2008).
[Eric03] John S. Erickson: *Fair use, DRM, and trusted computing*. Communications of the ACM, Volume 46, Issue 4 (April 2003).	[Eric03] John S. Erickson : *Fair use, DRM, and trusted computing*. Communication de l'ACM, volume 46, n° 4 (avril 2003).
[Gras06] Volker Grassmuck: *Wissenskontrolle durch DRM: von Überfluß zu Mangel*. Sammelband „Eigentum und Wissen". Jeanette Hofmann (Hrsg.), Bundeszentrale für Politische Bildung, Berlin 2006.	[Gras06] Volker Grassmuck : *Wissenskontrolle durch DRM: von Überfluß zu Mangel*. Ouvrage collectif « Eigentum und Wissen ». Jeanette Hofmann (dir.), Bundeszentrale für Politische Bildung, Berlin 2006.
[Gree07] Greene, T.: *Integrity of hardware-based computer security is challenged*. Network-World (2007). URL: http://www.networkworld.com/news/2007/062707-black-hat.html. Stand: 11.03.2009	[Gree07] Greene, T. : *Integrity of hardware-based computer security is challenged*. Network-World (2007). URL : http://www.networkworld.com/news/2007/062707-black-hat.html. (mise en ligne : 11.03.2009).
[GSS03] Dirk Günnewig, Ahmad-Reza Sadeghi, Christian Stüble: *Trusted Computing Platform Alliance* (Technical Report, 10/2003).	[GSS03] Dirk Günnewig, Ahmad-Reza Sadeghi, Christian Stüble : *Trusted Computing Platform Alliance* (rapport technique, 10/2003).
[Kaue07] Kauer, B.: OSLO: Improving the security of Trusted Computing. 16th USENIX Security Symposium (2007).	[Kaue07] Kauer, B. : OSLO: Improving the security of Trusted Computing. 16e Symposium USENIX Security (2007).
[KSP05] Kursawe, K., Schellekens, D., Preneel, B.: *Analyzing trusted platform communication*. (2005), URL: www.cosic.esat.kuleuven.be/publications/article-591.pdf	

[Pfit03] Roy Pfitzner: *TCPA, Palladium und DRM. Technische Analyse und Aspekte des Datenschutzes*. Technischer Report 2003.

[ReCa05] Reid, Jason F. and Caelli, William J.: *DRM, trusted computing and operating system architecture*. Conferences in Research and Practice in Information Technology Series; Vol. 108 Newcastle, New South Wales, Australia 2005

[Scha06] Jan Schallaböck, Ralf Bendrath, Udo Neitzel: *Privacy, Identity, and Anonymity in Web 2.0*. Präsentation vom: 27.12.2006. 23C3 Video Recordings URL: http://chaosradio.ccc.de/23c3_m4v_1611.html (Stand: Okt. 2008)

[Spie08] Bericht von *Spiegel-Online* vom 26.05.2008,
URL: http://www.spiegel.de/wirtschaft/0,1518,555491,00.html.

[Unis08] Bericht in der Zeitschrift *Unispiegel* vom 02.10.2008.

[KSP05] Kursawe, K., Schellekens, D., Preneel, B. : *Analyzing trusted platform communication*. (2005), URL : www.cosic.esat.kuleuven.be/publications/article-591.pdf.

[Pfit03] Roy Pfitzner : *TCPA, Palladium und DRM. Technische Analyse und Aspekte des Datenschutzes*. Rapport technique, 2003.

[ReCa05] Reid, Jason F. and Caelli, William J. : *DRM, trusted computing and operating system architecture*. Conférences « Recherche et pratique », dans la collection Information Technology Series; vol. 108 Newcastle, Nouvelle-Galles du Sud, Australie, 2005.

[Scha06] Jan Schallaböck, Ralf Bendrath, Udo Neitzel : *Privacy, Identity, and Anonymity in Web 2.0*. Présentation du 27.12.2006. 23C3 Enregistrements vidéo URL : http://chaosradio.ccc.de/23c3_m4v_1611.html (mise en ligne : octobre 2008).

[Spie08] Reportage du *Spiegel-Online*, 26.05.2008, URL :
http://www.spiegel.de/wirtschaft/0,1518,555491,00.html.

[Unis08] Reportage de la revue *Unispiegel*, 02.10.2008.