

Bundestrojaner & Co in der Strafverfolgung – Schutz der Privatsphäre im digitalen Zeitalter

Prof. Dr. Hans Kudlich¹

A. Die Digitalisierung unseres Lebens

Es hieße Eulen nach Athen tragen, wenn ich Ihnen zum Beleg für die Tatsache, dass wir im digitalen Zeitalter angekommen sind, hier noch einmal ausführlich die Durchdringung unseres gesamten Lebens durch moderne Informationstechnologien nachzeichnen würde. Nur ein kurzes und für uns alle hier anschauliches Beispiel soll genügen: Jedenfalls soweit ich für mich sprechen kann – und ich gehe davon aus, zumindest bei einigen von Ihnen war es ganz ähnlich – hat es im Zusammenhang mit der Einladung und Vorbereitung dieser Tagung kein einziges persönliches Gespräch und keinen einzigen auf Papier verfassten Brief gegeben. Einige wenige Dinge wurden telefonisch besprochen, der große Rest der Absprachen wurde per E-Mail getroffen. Im Vorfeld der Tagung ist nicht etwa ein Programm auf Papier verschickt worden, sondern das Tagungsprogramm findet sich im Internet wieder.

Nun geht es in den genannten Beispielen noch um relativ harmlose Daten. An ihnen hätten weder die Strafverfolgungsbehörden ein Interesse, noch hätte ich irgendwelche Schwierigkeiten damit, wenn öffentlich bekannt wird, dass ich an dieser Tagung teilnehme. Auf meinem Rechner zu Hause findet sich aber noch viel mehr, und dabei so manches, was doch etwas sensibler ist:

- meine Steuererklärung,
- im Zusammenhang mit Schreiben an die Krankenkasse Informationen zum Gesundheitszustand von mir und meiner Familie,
- private E-Mails, von denen ich nicht unbedingt wollen würde, dass Fremde sie lesen, und noch vieles mehr.

¹ Lehrstuhl für Strafrecht, Strafprozessrecht und Rechtsphilosophie, Friedrich-Alexander-Universität, Nürnberg-Erlangen. Der Vortragsstil wurde beibehalten, ebenso der „Rechtsstand“ vor der Entscheidung BVerfGE 120, 274; vgl. dazu *Kudlich*, JA 2008, 475 ff. Vertiefende Hinweise bei *Kudlich*, HFR (www.hunboldt-forum-recht.de) 2007, S. 202 ff.

B. Bedürfnis nach und Schwierigkeiten beim Schutz der Privatsphäre im digitalen Zeitalter

Wo so viele – teils mehr, teils weniger sensible – Daten anfallen, ist ein Schutz des Bürgers unumgänglich. Wenn wir vom „Schutz der Privatsphäre“ (oder wie auf anderen Tagungen: vom „Bürgerrechtsschutz“) im digitalen Zeitalter sprechen, so ist damit zweierlei gemeint:

1. Zum einen geht es um den Schutz des Bürgers *durch* den Staat. Dieser Schutz kann – nicht ausschließlich, aber auch – mit den Mitteln des Strafrechts erfolgen. Hier geht es um die Pönalisierung und anschließende Verfolgung von Computerkriminalität, also etwa von Phänomenen wie Hacking, „Datenklau“ oder Beeinträchtigung der Funktionsfähigkeit einer Computeranlage. Eine Reform der einschlägigen Strafnormen hat nicht nur in der Türkei, sondern gerade in der jüngeren Vergangenheit auch in Deutschland stattgefunden: Ein einschlägiges Reformgesetz, in dem insbesondere die Cyber Crime Convention sowie eine Richtlinie der Europäischen Union umgesetzt wurden, ist in diesen Tagen verabschiedet worden. Das soll aber heute nicht mein Thema sein.

2. Vielmehr geht es mir hier um den Schutz des Bürgers *vor* dem Staat, oder anders gewendet: Es geht um die Frage, welche (insbesondere grund-) rechtlichen Positionen im Auge behalten werden müssen, wenn die Strafverfolgungsbehörden moderne Ermittlungsmethoden anwenden, bei denen insbesondere auch neueste Informationstechnologie als Mittel oder als Gegenstand der Ermittlungen eine Rolle spielt.

a) Um dies vielleicht etwas plastischer zu machen, seien folgende – teilweise zumindest theoretisch denkbare, teilweise in der Strafverfolgungspraxis bereits häufig eingesetzte – Ermittlungsmaßnahmen genannt:

- Die Überwachung des ein- und ausgehenden E-Mail-Verkehrs bei einem Verdächtigen, vergleichbar der schon seit langem bekannten klassischen Überwachung des Fernmeldeverkehrs in Gestalt der traditionellen Sprachtelefonie.
- Sog. Side-Channel-Angriffe, bei denen die auf einem Rechner verarbeiteten Daten durch die elektromagnetischen Abstrahlungen bestimmter Hardware-Komponenten (insbesondere Bildschirme) verfolgt werden.
- Der Einsatz von sog. Key-Loggern, d.h. von Programmen, die an der Tastatur Eingaben eines Nutzers erfassen und an die Strafverfolgungsbehörden weiterleiten. Eine solche Maßnahme kann kriminalistisch attraktiv sein, weil

auf diese Weise z.B. Passwörter oder Schlüssel für verschlüsselte Kommunikationsvorgänge ermittelt werden können.

- Die Aktivierung von Hardware-Bestandteilen zur Raumüberwachung. Dabei werden eventuell am Computer des Verdächtigen angeschlossene Mikrophone oder Webcams – die angesichts der Popularität der Internettelefonie immer häufiger zu finden sind – durch eine entsprechende Ermittlungssoftware von außen aktiviert und zur Raumüberwachung genutzt.
- Last but not least: Die in Deutschland in den letzten Monaten intensiv diskutierte verdeckte Online-Durchsuchung, d.h. das – auf welchem Wege auch immer – Aufspielen einer Software auf dem Rechner eines Verdächtigen, welche die Festplatte durchsucht und während bestehender Internetverbindungen bestimmte Daten (z.B. Dokumente, archivierte E-Mails usw.) an die Strafverfolgungsbehörden übermittelt.

b) Bei all solchen Zugriffen mittels moderner Informationstechnologien oder insbesondere auf Computeranlagen durch die Strafverfolgungsbehörden handelt es sich um einen sehr sensiblen Bereich, der die Grundrechtsintensität des Eingriffs im Vergleich zum „Offline-Bereich“ nicht selten deutlich übertrifft. Dies hat verschiedene Gründe:

Zunächst können auf diese Weise u.U. große Datenmengen aus den verschiedensten Lebensbereichen gesammelt werden; Beispiele wie Informationen über den Vermögens- und Gesundheitsstand sowie verschiedenste private Kontakte wurden oben ja bereits genannt.

Ferner werden im Bereich der modernen Informationstechnologie in einem den meisten Nutzern nicht bekannten Umfang Datenspuren gelegt, die von den Strafverfolgungsbehörden auch noch ausgewertet werden können, wenn der eigentliche Vorgang schon längst abgeschlossen ist. Die kritische Diskussion um die sog. Vorratsdatenspeicherung, die auf Grund einer europäischen Initiative in Deutschland wohl kommen wird, zeigt das sehr deutlich.

Des Weiteren bieten sich elektronische Daten – nicht zuletzt aufgrund ihrer leichten Verarbeitbarkeit – hervorragend an, um diverse Verknüpfungen herzustellen. Darüber hinaus sind die elektronisch gesammelten Daten aber auch in besonders kritischer Weise für Missbräuche anfällig. Dabei soll es an dieser Stelle nicht einmal so sehr um den Missbrauch durch die Strafverfolgungsbehörden gehen, sondern um drohende Missbrauchspotentiale, wenn die Daten – denn auch die Systeme der Strafverfolger haben Schwachstellen – etwa in die Hände krimineller Vereinigungen geraten.

Zuletzt liegt eine besondere Intensität des Eingriffs darin, dass er nicht selten heimlich, d.h. ohne Wissen des Betroffenen erfolgen kann. Insbesondere die fehlende sinnliche Wahrnehmbarkeit entsprechender Aktionen sowie die leichte Kopierbarkeit elektronischer Daten führen dazu, dass sich der „gläserne Bürger“ seiner Durchsichtigkeit oft gar nicht bewusst sein wird.

All diese Aspekte – Sammlung großer Datenmengen, leichte Verknüpfbarkeit und nicht-offene Ermittlungsmöglichkeiten – stellen aus Sicht der Strafverfolgungsbehörden natürlich kriminaltaktische Vorteile dar, die eine effiziente Strafverfolgung im Einzelfall besonders fördern können. Aus Sicht des Bürgers jedoch sind es schwerwiegende Gefahren.

c) Hinzu treten rechtliche Probleme:

So handelt es sich bei Ermittlungsmaßnahmen im Internet und anderen modernen Informationstechnologien um relativ neue Phänomene, zu denen viele Rechtsfragen im Einzelnen noch ungeklärt sind.

Eine solche Klärung wird dabei noch dadurch erschwert, dass die meisten strafprozessualen Ermittlungsbefugnisse in einer Zeit formuliert worden sind, in der die heutigen technischen Entwicklungen noch nicht einmal erahnt werden konnten. Aber sogar dann, wenn – wie in den letzten Jahren mehrfach erfolgt und momentan in einer großen Strafprozessrechts-Reform gerade in Planung – die einschlägigen Vorschriften neu formuliert werden, hinkt der Gesetzgeber in dieser dynamischen Materie fast zwangsläufig schon nach kurzer Zeit den technischen Realitäten mehr oder weniger hinterher.

Ferner wird eine Klärung dadurch erschwert, dass insbesondere die grundrechtliche Zuordnung verschiedener Maßnahmen bzw. verschiedener schützenswerter Rechtspositionen schwierig ist. Das hängt mit der für das Internet typischen Konvergenz der klassischen Medien zusammen. Ist es z.B. die Überwachung des E-Mail-Verkehrs eine Überwachung der Telekommunikation (obwohl E-Mails doch so wenig mit dem Telefonieren zu tun haben, wie wir es vorher gekannt haben) oder ist es vielleicht eher eine Postbeschlagnahme? Diese schwierigen Einordnungsfragen beschäftigen die Rechtswissenschaft, seit in den 90er Jahren die ersten Regelungen für das Phänomen Internet geschaffen worden sind: So beruhte etwa das lange Zeit bestehende Nebeneinander des Teledienstgesetzes und des Mediendienste-Staatsvertrags auf der Einordnungsfrage, was „das Internet“ überhaupt ist: Ist es ein Fall der Individualkommunikation? Hat es mit Rundfunk zu tun? Oder ist es eher mit der Presse vergleichbar? Das Medium entzieht sich gewissermaßen unseren gewohnten Denkkategorien und damit auch unseren gewohnten rechtlichen Kategorien.

Beide Aspekte – die Neuartigkeit der Fragestellung und die schwierige grundgesetzliche, aber auch sonstige rechtliche Zuordnung – fördern vielleicht auch eine gewisse Tendenz, die man m.E. in diesem Bereich feststellen kann: Die Tendenz der Strafverfolgungsbehörden nämlich, die Durchführung entsprechender Maßnahmen „einfach einmal zu versuchen“. Entsprechende Maßnahmen sind schnell beantragt, und man kann im Einzelfall durchaus „Glück“ haben und auf einen Ermittlungsrichter treffen, der sie ohne großes Nachdenken anordnet. Dabei wird dann die – im Grundsatz gar nicht zu bestreitende – „Entwicklungsoffenheit“ strafprozessualer Befugnisnormen dahingehend missverstanden, dass jede Ermittlungsmaßnahme eben einfach unter die Befugnis „gepackt“ werden kann, die noch am ehesten dazu zu passen scheint. Eine genaue, am Vorbehalt des Gesetzes für Grundrechtseingriffe orientierte Rechtsanwendung im Einzelfall findet dann oft nicht mehr statt.

Geradezu bezeichnend für dieses Vorgehen sind gewisse Begründungstendenzen, die in diesem Bereich zu verschiedenen Phänomenen in der Rechtsprechung zu finden sind: Insbesondere bei der Anwendung der Vorschriften über die Überwachung der Telekommunikation nach § 100a in der Strafprozessordnung neigen die Strafverfolgungsbehörden mitunter dazu, alles, was irgendwie unter einen weiten Begriff der Telekommunikation gefasst werden kann, mittels der Vorschrift des § 100a StPO überwachen zu lassen. Dabei wird dann gerne auch das Argument herangezogen, dass der Begriff der Telekommunikation aufgrund des Schutzes des Fernmeldegeheimnisses in Art. 10 GG weit ausgelegt werden müsse, um diesem Grundrecht Geltung zu verschaffen. Dabei wird – bewusst oder unbewusst – übersehen, dass eine mögliche grundrechts-effektuiierende weite Auslegung eines Merkmals nicht notwendig auch mit der gleich weiten Auslegung einer strafprozessualen Eingriffbefugnis korrespondieren muss. Oder anderes gewendet: Die Tatsache, dass eine bestimmte Ermittlungsmaßnahme thematisch irgendwie in den Anwendungsbereich eines Grundrechtes gehört, führt nicht automatisch dazu, dass die Ermittlungsbefugnis, die Eingriffe in den Schutzbereich dieses Grundrechtes rechtfertigen kann, automatisch auch einschlägig ist. Andersherum wird ein Schuh daraus: Gerade weil durch eine weite Auslegung des Begriffs der Telekommunikation ein Eingriff in den Schutzbereich des Art. 10 GG vorliegt, muss im Einzelfall geprüft werden, *ob* auch eine entsprechende Rechtfertigung besteht.

C. Das Beispiel der Online-Durchsuchung

1. An einem konkreten Fall exemplifiziert seien die eher abstrakt umrissenen Probleme am Beispiel eines Falles, der in Deutschland in den letzten Monaten zu einigem Gesprächsstoff geführt hat, der sog. verdeckten Online-Durchsuchung, auch

bekannt geworden im Zusammenhang mit der Bezeichnung der präsumtiv zu verwendenden Software als „Bundestrojaner“.

Dabei ging es um Folgendes: In einem Ermittlungsverfahren mit terroristischem Hintergrund beantragte der Generalbundesanwalt beim Ermittlungsrichter des Bundesgerichtshofs die Durchsuchung eines vom Beschuldigten benutzten Computers anzuordnen und den Ermittlungsbehörden zur verdeckten Ausführung gewisse Maßnahmen zu gestatten, ein hierfür konzipiertes Computerprogramm – eben jenen Bundestrojaner – dem Beschuldigten zur Installation zuzuspielen, um die auf dem Computer abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen. Nachdem der Ermittlungsrichter des Bundesgerichtshofs – anders als noch ein knappes Jahr vorher ein anderer Ermittlungsrichter – die Durchführung dieser Maßnahme abgelehnt und auch der Beschwerde der Generalbundesanwaltschaft nicht abgeholfen hatte, befasste sich der 3. Strafsenat des Bundesgerichtshofs mit dieser Frage und lehnte die Gestattung einer solchen verdeckten Online-Ermittlung ebenfalls ab.

In der Sache ist diese Entscheidung – jedenfalls *de lege lata* – gewiss richtig: Es handelt sich bei der „verdeckten Online-Durchsuchung“ eben um keine Durchsuchung im Sinn der Strafprozessordnung, da eine solche – das ergibt sich aus einer Reihe von Vorschriften – grundsätzlich ein „offenes“ Tätigwerden der Strafverfolgungsbehörden vor Augen hat. Hinzu kommt, dass die Eingriffsintensität der geplanten Online-Durchsuchung auch deswegen größer wäre, weil nicht nur – wie bei der traditionellen Durchsuchung – eine Bestandsaufnahme zu einem bestimmten Zeitpunkt geliefert werden kann, sondern die Durchsuchung auch über einen längeren Zeitraum hinweg erfolgen würde. Ebenso wenig handelt es sich – jedenfalls bei einer Vielzahl von auf dem Rechner gespeicherten Dokumenten – auch um eine Überwachung der Telekommunikation, da diese die Überwachung des jeweils in Gang befindlichen Kommunikationsvorganges vor Augen hat, nicht etwa den Zugriff auf jeglichen elektronisch erstellten Inhalt. Dass die Übertragung der Daten an die Strafverfolgungsbehörden jeweils nur erfolgen kann, wenn der Betroffene gerade mit dem Internet verbunden ist, kann daran natürlich nichts ändern; denn die einzige Echtzeit-Kommunikation, die dabei zur Kenntnis genommen würde, wäre ja die vom Bundestrojaner initiierte Datenübertragung an die Verfolgungsbehörden.

Zuletzt ist dem Bundesgerichtshof auch darin zuzustimmen, dass eine solche Maßnahme nicht gleichsam in einer Art „Zusammenschau“ verschiedener Ermittlungsbefugnisse oder im Wege der Analogie gerechtfertigt werden kann, sondern dass der auch für Ermittlungsmaßnahmen im Strafverfahren geltende grundgesetzliche Gesetzesvorbehalt eine klare gesetzliche Grundlage verlangt.

2. Auch wenn dem Bundesgerichtshof hier uneingeschränkt zuzustimmen ist und die Sache damit im konkreten Fall „gut ausgegangen“ ist, macht der Fall noch einmal sehr schön die oben genannten Probleme deutlich: Es besteht eine erhebliche Rechtsunsicherheit, denn immerhin hatten der Generalbundesanwalt und einige Monate vorher auch ein anderer Ermittlungsrichter des Bundesgerichtshofs die verdeckte Online-Durchsuchung für zulässig gehalten. Die korrekte Zuordnung der betroffenen Grundrechte bereitet gewisse Schwierigkeiten. Und auch das oben beschriebene Phänomen „man kann es ja mal versuchen“ ist in dem wie selbstverständlich gestellten Antrag und der gegen die erste Entscheidung des Ermittlungsrichters sogar noch eingelegten Beschwerde der Generalbundesanwaltschaft sehr deutlich geworden.

De lege lata ist das Problem nunmehr aber durch den Bundesgerichtshof befriedigend gelöst und muss deswegen vorliegend nicht mehr vertieft werden. Interessanter ist dagegen das, was möglicherweise de lege ferenda passiert und was dabei zu beachten ist: Bundesinnenminister Schäuble – zu dessen Zuständigkeit allerdings in erster Linie die präventivpolizeiliche und nicht die kriminalpolizeiliche Arbeit gehört und der insoweit in der Justizministerin Zypries eine hartnäckige Widersacherin hat – hat sich rasch für die Schaffung einer entsprechenden gesetzlichen Grundlage ausgesprochen. Das gleiche gilt für das Bundeskriminalamt. Im Bundesrat ist bereits ein Antrag des Freistaats Thüringen zu einer Entschließung zur Schaffung einer Rechtsgrundlage für verdeckte Online-Durchsuchungen im Strafverfahren eingegangen. Zwar hat eine entsprechende Regelung noch keinen Eingang in die momentan im Bundestag diskutierte Reform der Strafprozessordnung im Bereich der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen gefunden; ob sich hierzu aber nicht im Laufe des Gesetzgebungsverfahrens noch etwas ergibt, ist aus meiner Sicht gegenwärtig offen. Und für den präventivpolizeilichen Bereich ist im Verfassungsschutzgesetz des Landes Nordrhein-Westfalen bereits eine entsprechende Regelung aufgenommen worden (gegen die gegenwärtig auch schon die erste Verfassungsbeschwerde anhängig ist).

3. Dass eine entsprechende Regelung zur Online-Durchsuchung früher oder später kommen wird, erscheint mir nahe liegend. Ihre kriminaltaktischen Vorteile liegen auf der Hand. Unabhängig davon aber, wie sie im Detail aussehen wird, bietet eine solche hypothetische Regelung ein gutes Beispiel, insbesondere für die schwierige Grundrechtszuordnung bei modernen Ermittlungsmaßnahmen. Verschiedene Grundrechte stehen im Raume; welches davon – überhaupt oder jedenfalls vorrangig – einschlägig ist, ist dagegen umstritten.

a) Die mit Blick auf eine Schaffung einer gesetzlichen Regelung spannendste Frage liegt darin, ob bzw. wann eine heimliche Online-Durchsuchung den Schutzbereich des

Grundrechts auf Unverletzlichkeit der Wohnung nach Art. 13 GG berühren kann. Dies ist deshalb interessant, weil Art. 13 GG in seiner gegenwärtigen Fassung keinen Gesetzesvorbehalt für strafprozessuale Maßnahmen außerhalb der klassischen Durchsuchung und des großen Lauschangriffs enthält, so dass eine entsprechende Befugnisnorm entweder verfassungswidrig wäre oder aber auch eine Verfassungsänderung voraussetzt.

Das Grundrecht auf Unverletztheit der Wohnung aus Art. 13 GG verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in diesem Raum in Ruhe gelassen zu werden. Es enthält das an die öffentliche Gewalt gerichtete Verbot, gegen den Willen des Wohnungsinhabers in die Wohnung einzudringen, nach der Rechtsprechung des Bundesverfassungsgerichts aber auch das grundsätzliche Verbot, etwa Abhörgeräte in der Wohnung zu installieren. Damit schützt Art. 13 GG nicht nur gegen die unerwünschte physische Anwesenheit eines Vertreters der Staatsgewalt, da die heutigen technischen Möglichkeiten es erlauben, in die geschützte räumliche Sphäre auch anders einzudringen. Der Schutzzweck des Grundrechts würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel nicht umfasst wäre, nur weil sie außerhalb der Wohnung eingesetzt werden.

Dennoch wird von einer verbreiteten, und vielleicht sogar herrschenden Meinung – m.E. allerdings zu Unrecht – die Einschlägigkeit des Art. 13 bei der Online-Durchsuchung abgelehnt. Dies wird damit begründet, es sei Zweck des Grundrechts auf Unverletzlichkeit der Wohnung den Staat aus der Wohnung, nicht aber „aus dem Rechner“ herauszuhalten. Auch bringe die Online-Durchsuchung regelmäßig keine Informationen über Vorgänge in der Wohnung mit sich. Insbesondere aber führe der Anschluss eines Rechners an das Internet dazu, dass – wenn schon keine subjektive Einwilligung, so doch jedenfalls – eine Änderung der „objektiven Kommunikationsbedingungen“ dergestalt eintrete, dass diese nunmehr gewissermaßen „offen“ würden. Trotz der räumlichen Abschottung der Wohnung könne jetzt mit dem Computer mit der Außenwelt kommuniziert wie umgekehrt aus dem Netz grundsätzlich auf den Computer zugegriffen werden. Mit dem Anschluss an das Internet entstehe also ein gegenüber der Wohnung eigenständiger „virtueller Raum“. Sobald man „online gehe“, könne man auf den Schutz des Wohnungsgrundrechts nicht länger vertrauen; die durch Firewalls oder sonstige Vorkehrungen geschaffenen „virtuellen Räume“ würden dagegen nicht in den Schutzbereich des Art. 13 GG fallen.

Richtigerweise ist demgegenüber davon auszugehen, dass der Schutzbereich des Art. 13 GG jedenfalls dann betroffen ist, wenn der von der Online-Durchsuchung betroffene Rechner in einer Wohnung steht.

Das Argument der angeblichen „Öffnung der objektiven Kommunikationsbedingungen“ durch den Anschluss an das Internet ist ersichtlich unsinnig. Zum einen ist schon nicht zu vermitteln, warum eine solche „virtuelle Öffnung“ von Bedeutung, ein „virtueller Raum“ kraft Firewalls etc. dagegen unbeachtlich sein soll. Vor allem aber wird auch sonst durch eine Öffnung der Wohnung gegenüber solchen Personen, die mit Wissen und Wollen des Wohnungsinhabers eintreten, der räumliche Schutz im Übrigen nicht tangiert.

Vielmehr muss Art. 13 GG auch die Verfügungsbefugnis darüber schützen, welche Informationen aus der Wohnung eigenmächtig „entnommen“ werden. Anders als von der Gegenmeinung propagiert, stellt die Wohnung eben dennoch eine zusätzliche räumliche Abschottung dar. Zwar ist es im Einzelfall ohne Zweifel Zufall, ob der Nutzer innerhalb oder außerhalb seiner Wohnung (etwa in einem Internetcafe oder an einem Hot Spot) „online geht“ – diese Zufälligkeit spricht aber nicht gegen eine Einbeziehung in den grundrechtlichen Schutzbereich. Vielmehr ist es bei allen Gegenständen in diesem Sinne vom Zufall abhängig, ob sie sich in einer Wohnung befinden (und dem Zugriff darauf dann unter Umständen Art. 13 GG entgegensteht) oder außerhalb der Wohnung. Das dürfte im Übrigen auch dem heute noch vorherrschenden Verständnis des Verhältnisses zwischen festen und mobilen Anschlüssen im Internet entsprechen: In der deutschen Sprache ist etwa für ein Notebook – und umso mehr für ein solches, mit dem man außerhalb der eigenen Sphäre „online geht“ – das Bild des „mobilen Büros“ gebräuchlich; dagegen kommt eigentlich niemand auf die Idee, in einem zu Hause installierten Computer ein potentiell mobiles Medium zu sehen, das gewissermaßen nur akzidentiell dauerhaft an einem Ort installiert ist.

b) Demgegenüber ist – auf den ersten Blick vielleicht überraschend – der Schutzbereich des Fernmeldegeheimnisses nach Art. 10 GG bei der Online-Durchsuchung zumindest regelmäßig nicht betroffen. Denkbar ist die Einschlägigkeit der Telekommunikationsfreiheit von vornherein nur bei Dokumenten, die über einen Kommunikationsvorgang erhalten worden sind (insbesondere E-Mails), und auch hier wohl nur, solange der Kommunikationsvorgang noch nicht abgeschlossen ist. Eine Ausnahme wird mitunter angenommen, soweit durch die Online-Durchsuchung letztlich nur der Schlüssel für weitere verschlüsselte Kommunikationsvorgänge (z.B. im E-Mail- oder Telefonverkehr) aufgefunden werden soll, weil hier ein unmittelbarer innerer Zusammenhang mit der späteren geplanten Überwachung der Telekommunikation bestehen soll. Freilich erscheint mir ein solcher Zusammenhang deutlich konstruierter als etwa die hier befürwortete Annahme, ein in der Wohnung befindlicher PC falle unter den Schutz des Art. 13 GG.

c) Lehnt man – was relativ unstrittig sein dürfte – zumindest grundsätzlich die Einschlägigkeit des Telekommunikationsgeheimnisses ab und sieht man – entgegen der hier vertretenen Auffassung – grundsätzlich auch Art. 13 GG als nicht einschlägig an, so bleibt nur noch das so genannte Recht auf informationelle Selbstbestimmung. Dieses wurde vom Bundesverfassungsgericht im bekannten Volkszählungsurteil im 65. Band der Amtlichen Sammlung als Ausfluss der Menschenwürde und des Persönlichkeitsrechtes nach Art. 2 Abs.1 Satz 1 GG entwickelt.

Viele, wenn nicht sogar die meisten auf einem Computer befindlichen Daten dürften über die entsprechende Zuordnung zur Person des Nutzers personenbezogene Daten sein, deren Abruf einen Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung darstellt. Ob und wann dieser Eingriff im Einzelfall gerechtfertigt wäre, hängt zum einen von der konkreten Ausgestaltung der Befugnisnorm, zum anderen von der Gestaltung des jeweiligen Ermittlungssachverhaltes ab, vor allem aber auch vom Inhalt des jeweiligen Dokuments ab. Befinden sich – ohne weiteres vorstellbar – auf dem Rechner tagebuchartige Aufzeichnungen (und gemeint sind hier: solche, die nicht in der heute vielfach zu beobachtenden Gedankenlosigkeit gerade junger Nutzer in geradezu exhibitionistischer Manier online jedermann zugänglich gemacht werden), so kann man sich rasch dem Kernbereich der Intimsphäre nähern, in den auf Grund des Menschenwürdegehalts Eingriffe nicht oder nur unter sehr engen Voraussetzungen möglich sind.

Wichtiger als diese Detailfragen scheinen mir im Zusammenhang mit dem Grundrecht auf informationelle Selbstbestimmung aber generelle Erwägungen zu sein: Wenn man sich mit der Einschlägigkeit dieses Grundrechtes tröstet und deshalb leichten Herzens die Einschlägigkeit des Wohnungsgrundrechtes ablehnt (und dann wohl erst recht die Frage nach einer wohnungsähnlichen Ausweitung des Schutzes von Computer- und Kommunikationsdaten *de constitutione ferenda* weit von sich weisen muss), bagatellisiert man m.E. den Eingriff. Dem Recht auf informationelle Selbstbestimmung wird in anderen Zusammenhängen nicht zu Unrecht bisweilen der Vorwurf einer Hypertrophie gemacht. Mit ihm wird versucht, auch mehr oder weniger marginalen Persönlichkeitsbeeinträchtigungen die besondere Weihe des Grundrechtsseingriffs zu verleihen. Werden nun etwa Videoaufnahmen von Überwachungskameras auf öffentlichen Bahnsteigen hinsichtlich der Intensität des Grundrechtseingriffs mit der heimlichen Online-Durchsuchung in privaten Daten (zumindest scheinbar) gleichgesetzt, so fehlt hier jedes Maß.

D. Übergeordnetes Problem: Schutz des Kernbereichs privater Lebensgestaltung

Der soeben angesprochene Gesichtspunkt, dass gerade bei der verdeckten Online-Ermittlung auf viele in hohem Maße persönlichkeitsrelevante Informationen bis hin zu tagebuchartigen Aufzeichnungen zurückgegriffen werden kann, führt zu einem übergeordneten Problem, das nicht nur bei der Online-Durchsuchung, sondern auch bei anderen Überwachungsmaßnahmen – und streng genommen nicht einmal nur bei Überwachungsmaßnahmen mit Mitteln der modernen Informationstechnologie – auftritt:

Das Bundesverfassungsgericht hat im Jahr 2004 in einer Entscheidung zur Zulässigkeit der Überwachung des nicht-öffentlich gesprochenen Wortes in Wohnräumen (sog. großer Lauschangriff) darauf hingewiesen, dass auch bei der Verfolgung von Straftaten der Kernbereich der privaten Lebensgestaltung gewahrt werden muss. Dieser Kernbereich kann (außer etwa in den „Tagebuchfällen“) insbesondere auch bei der Kommunikation mit Vertrauenspersonen betroffen sein, welcher dann im Einzelfall nicht überwacht werden darf bzw. deren Überwachung gerichtlich nicht verwertet werden darf. In der oben angesprochenen Reform der StPO mit Blick auf nicht-offene Ermittlungsmethoden ist diese verfassungsgerichtliche Forderung in verschiedener Weise aufgegriffen worden. Im Einzelfall scheint die Umsetzung allerdings schwierig und sorgt schon jetzt für einigen Gesprächsbedarf. Dazu zwei Beispiele:

In dem eingangs erwähnten Verfassungsschutzgesetz des Landes Nordrhein-Westfalen fehlen hinsichtlich der heimlichen Online-Durchsuchung entsprechende Sperrbestimmungen bzw. Verwertungsverbote vollständig. Der nordrhein-westfälische Gesetzgeber steht auf den Standpunkt, diese Einschränkungen würden nur für den Bereich der akustischen Wohnraumüberwachung gelten – eine Vorstellung, die evident halbwegs naiv ist.

Zum anderen sind bereits jetzt Klagen der Lobbyisten – etwa der Interessenvertreter der Wirtschaftsprüfer und Ärzte – laut geworden, warum für bestimmte Berufsgruppen nur relative Beweisverbote – nämlich bei einem Nachweis der Berührung des Kernbereichs der privaten Lebensgestaltung im konkreten Einzelfall – angenommen werden, während bei anderen Berufsgruppen (insbesondere bei Strafverteidigern, weniger plausibel übrigens auch bei Seelsorgern und Parlamentariern) – eine Beziehung zum Kernbereich der privaten Lebensgestaltung gleichsam vermutet wird. Diese Klagen überraschen, weil das Schutzniveau des Verhältnisses zwischen den entsprechenden Berufsträgern und ihren „Kunden“ (also etwa Patienten bzw. Mandanten) gegenüber der bisherigen Rechtslage auf jeden Fall gestärkt worden ist.

E. Ausblick und Fazit

In der Kürze der Zeit konnte notwendig nur ein sehr grober und anhand eines einzelnen, in der deutschen Diskussion gegenwärtig ausgesprochen prominenten Beispiels vertiefter Überblick über das Problem des Schutzes der Privatsphäre bei den Ermittlungen der Strafverfolgungsbehörden im digitalen Zeitalter gegeben werden. Wesentliche strukturelle Schwierigkeiten, hier die Balance zwischen Strafverfolgung und Grundrechtsschutz nicht zu verlieren, sind deutlich geworden. Ein „wer nichts zu verbergen hat, hat auch nichts zu befürchten“-Ansatz ist sicher nicht hilfreich und kaum geeignet, das Vertrauen der Bevölkerung in die modernen Kommunikationsmittel, aber auch in die staatliche Hoheitsgewalt zu stärken.

Andererseits sollte man aber auch nicht zu schwarzsehen: Gerade die letztgenannte kleine Anekdote der Klagen der Wirtschaftsprüfer und Ärzte über eine angebliche Benachteiligung im Rahmen der StPO-Reform machte deutlich, dass in Deutschland mitunter „auf hohem Niveau gejammert“ wird. Manche vermeintlichen Schwierigkeiten ergeben sich überhaupt erst bei dem Versuch, dem doch relativ hohen Schutzniveau durch das deutsche Grundgesetz gerecht zu werden, ohne eine an die Realitäten der modernen Kriminalität angepasste effektive Strafverfolgung von vornherein auszuschließen. Wer überall nur Gefahren und staatliche Missbräuche sieht, wird immer und an jeder Regelung ein Haar in der Suppe finden. Man stelle sich nur einmal vor, im Klima eines derartigen Misstrauens müsste heute noch einmal die Frage diskutiert werden, ob – was tägliche Praxis ist – körperliche Eingriffe in Gestalt einer Blutentnahme zur Aufklärung von Bagatelldelikten im Bereich des Straßenverkehrs angeordnet werden sollen. Ein Missbrauchspotential besteht auch bei abgenommenem Blut – man denke nur an die Durchführung heimlicher flächendeckender Gentests und den Aufbau entsprechender Dateien... Zumindest soweit wir wissen, sind trotz der vergleichsweise langen Geschichte derartiger Blutentnahmen solche Auswüchse bisher unterblieben. Bei aller gebotenen Wachsamkeit und aller Sensibilität für drohende Grundrechtseingriffe sollten wir uns also einen letzten Rest Optimismus erhalten.

Ceza Kovuşturmasında Federal Truva Atları – Dijital Çağda Özel Yaşam Alanının Korunması

Prof. Dr. Hans Kudlich¹

Übersetzt von: Rabia Ünlü, LL.M.Eur.

A. Hayatımızın Dijitalleştirilmesi

Dijital çağda yaşadığımız iletişim teknolojilerin tüm hayatımıza iyiden iyiye nasıl dahil olduğu gerçeğini ispat etmek, herhalde tereciye tere satmaya benzeyecektir. Kısa ve hepimiz için anlaşılır bir örnek yeterli olacaktır: Bildiğim kadarıyla bu sempozyumun hazırlıklarında (ki, sizde de farklı olduğunu düşünmüyorum), ne el yazısıyla yazılan bir mektup gönderilmiştir, ne de bir telefon görüşmesi yapılmıştır. Sadece bazı küçük şeyler telefonla, geri kalan işler ise çoğunlukla elektronik posta yoluyla halledilmiştir. Sempozyum programı önceden kağıda basılarak gönderilmek yerine, internet ortamında herkese ulaştırılmıştır.

Bu örnekler internet ortamında henüz masum sayılan verilerdir. Bu bilgiler, ne ceza kovuşturma organlarının ilgisini çekecek, ne de bir sempozyuma katılacağıma dair bilginin yayınlanması beni rahatsız edecek niteliktedir. Evimdeki bilgisayarımda ise çok daha hassas veriler mevcuttur, örneğin:

- Şahsıma ait vergi beyannamesi,
- Sigortama göndereceğim, ailemin sağlık durumuyla ilgili bilgiler içeren bir yazı,
- Yabancı şahısların eline geçmesini istemediğim özel e-mailler.

B. Dijital çağda özel yaşam alanının korunmasına duyulan ihtiyaç ile bunun zorlukları

Hassas olan ve olmayan bu kadar çok sayıda veri söz konusu olduğunda, vatandaşın korunması kaçınılmaz olmaktadır. Başka sempozyumlarda, vatandaşlık haklarının

¹ Ceza Hukuku, Ceza Muhakeme Hukuku ve Hukuk Felsefesi kürsüsü, Friedrich-Alexander Üniversitesi, Nürnberg-Erlangen. Sunum tarzı BVerfGE 120, 274 karar'ın hukuki durumu ile aynı kalmıştır; karşı: Kudlich, JA 2008, 475 ff. Ayrıntılı bilgi için bkz.: Kudlich, HFR (www.humboldt-forum-recht.de) 2007, S. 202 vd.

korunması olarak tabir ettiğimiz, dijital çağda özel yaşam hakkının korunmasından bahsediyorsak eğer bunu iki farklı açıdan değerlendirmek gerekecektir.

Öncelikle vatandaşın *devlet tarafından* korunmasını ele almak gerekir. Bu koruma başka kanunların yanı sıra, ceza kanunu aracılığıyla da sağlanabilmektedir. İlgili kanun maddeleri hacking, veri hırsızlığı veya bilgisayarın çalışma düzenini etkileme gibi bilişim suçlarının öncelikle izinin bulunmasını ve ardından takip edilmesini öngörmektedir. Bu konuyla ilgili sadece Türk Ceza Kanununda değil Siber Suç Sözleşmesinde ve Avrupa Birliği tavsiye kararında yer alan maddelerin, Alman Ceza Kanununa uyarlanmasını öngören bir uyum kanununun bugünlerde yürürlüğe konmasıyla, Alman Ceza Kanununda da bir yasa değişikliğine gidilmiştir. Fakat bugün bu konuya değinmeyeceğiz.

Burada ağırlık verdiğim konu daha çok, vatandaşın *devletten* korunmasıdır veya bir soruyla ifade etmek gerekirse: Ceza kovuşturma organlarının, modern soruşturma yöntemlerini, özellikle de bilgi işlem teknolojisinin ürettiği en son alet ve araçları kullanmaları halinde, hangi yasal ve anayasal pozisyonları göz önünde tutmaları gerekir.

a) Bunu somutlaştırmak adına, teorik olarak mümkün olan ve kısmen ceza kovuşturması uygulamalarında kullanılan soruşturma yöntemlerini sunmak gerekecektir:

- Klasik sayılan ve uzun zamandır bilinen, telefon konuşmalarının gizlice dinlenmesinin bilişim sistemindeki karşılığı olan, şüphelinin e-mail yoluyla yapılan yazışmalarının takip altına alınması.
- Bilgisayar donanım birimlerinin her birinin, özellikle de bilgisayar ekranının, yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesi tekniğinin kullanıldığı Side-, Channel- saldırıları.
- Bir kullanıcının bilgisayarına klavye yoluyla aktardığı her türlü verileri kaydeden ve cezai kovuşturma organlarına aktaran “key logger” programlarının kullanılması. Şifrelerin ve şifreli iletişim işlemlerinin takip edilmesini kolaylaştıran bu tarz bir yöntem kriminolojik açıdan da incelemeye değer olabilir.
- Odayı gözetleme amacıyla Hardware bileşenlerinin uzaktan aktive edilmesi. internet yoluyla telefon görüşmelerinin gitgide yaygınlaşmasıyla, birçok kişinin bilgisayarında bağlı olan bir mikrofon veya bir webcam şüphelinin bilgisayarında da mevcut ise, bir arama programının uzaktan aktive edilmesiyle odanın gözetlenmesi veya dinlenmesi mümkün olacaktır.

- Son olarak, Almanya’da yoğun olarak tartışılan gizli online arama işlemi. Yani şüphelinin bilgisayarına ne şekilde olursa olsun bir programın yüklenmesi ve bu program sayesinde harddisk üzerinde kayıtlı verilerin taranması ve ardından internet bağlantısı olduğu süre içerisinde verilerin (önceden kaydedilmiş e-mail yazışmaları veya belgeler gibi) ceza kovuşturması organlarına aktarılması.

b) Modern bilgi işlem teknolojileri aracılığıyla yapılan her türlü müdahale, özellikle de ceza kovuşturması organlarınca bilgisayarlara yapılan müdahaleler, kişinin temel hak ve özgürlüklerine etkisi açısından, internetin kullanılmadığı alandan çok daha hassas bir alan teşkil etmektedir. Bunun farklı sebepleri vardır:

Öncelikle bu yöntemle, kişinin farklı yaşam alanlarından çok sayıda veri toplanabilir, örneğin yukarıda da belirttiğim gibi kişinin malvarlığı, sağlık durumu ve şahsi çevresiyle ilgili bilgiler gibi.

En son bilgi teknolojisi sayesinde geçmişte yapılan tüm işlemler, bu işlemler sonradan silinmiş olsa dahi, bir yerde izleri kaydedilmiş olup, ceza kovuşturması organları, bilgisayar kullanıcılarının, boyutunun ne kadar olduğu pek bilinmeyen geçmişte yaptıkları işlemlerin izlerini bulup değerlendirebilmektedir. Avrupa Birliğinin bir girişimiyle Almanya’ya da gelecek olan yedek veri arşivi uygulamasıyla ilgili tartışmalar bu yöntemin en iyi ispatıdır.

Bunun dışında, üzerinde işlem yapılması kolay olduğundan, elektronik veriler, bazı önemli bağlantılar kurmak için çok elverişli olduğu kadar, elektronik ortamda toplanan veriler kötüye kullanılmaya da son derece elverişlidir.

Son olarak bu tarz bir müdahaleye maruz kalan şahsın bundan habersiz olması müdahalenin şiddetini arttırmaktadır. Kişinin algılaması mümkün olmayan bu müdahaleler ve elektronik verilerin kolayca kopyalanabilir olması, farkında olmadan vatandaşın “şeffaflaşmasına” sebep olmaktadır.

Tüm bu sayılan çok sayıda verilerin toplanılması, kolay yoldan bağlantıların yapılabilmesi ve soruşturmanın gizlice yapılması olanağı gibi faktörler, ceza kovuşturması organlarına göre kriminolojik açıdan büyük avantajlar sağlamakta ve etkili bir suç kovuşturmasını desteklemektedir. Fakat vatandaş açısından büyük tehlikeler arz etmektedir.

- c) Bundan ziyade hukuki bir takım sorunları da beraberinde getirmektedir:

İnternet yoluyla veya en son bilgi teknolojilerinin sunduğu imkanlarla yapılan soruşturma yöntemleri daha çok yeni sayılır ve beraberinde getirdiği bir çok hukuki sorunlara henüz cevap bulunamamıştır.

Ceza Muhakemesi Yasasının kovuşturma yetkileriyle ilgili çoğu maddelerinin, bugünkü teknolojik imkanlarının tahmin dahi edilemeyen bir zamanda yazılmış olması da, bu sorunların giderilmesini bir o kadar zorlaştırmaktadır. Bugün gerekli olan yasa değişiklikleri yapılsa dahi (ki, son yıllarda bazı değişiklikler yapılmıştır ve halihazırda büyük bir Ceza muhakemesi Yasası reformu planlanmaktadır) kısa bir süre sonra konunun dinamik yapısı gereği teknolojik gerçekliklerle uyum sağlamayacak ve yeni reformlar gerektirecektir.

Ayrıca korunması gereken farklı hukuki pozisyonlar ile bahse konu bu yöntemlerin temel hak ve özgürlükler açısından yerlerinin belirlenmemiş olması, sorunların çözümünü zorlaştırmaktadır. Bu da internetin klasik medya araçlarıyla benzer hale gelmiş olmasından kaynaklanmaktadır. Örneğin e-mail yazışmalarının takip altına alınması telekomünikasyon araçlarının takip edilmesiyle mi (oysa ki e-mail yazışmaları telefon görüşmelerinden farklıdır) yoksa mektupların okunmasıyla mı eşdeğer tutulabilir? Bu tarz bir tanımlama ve konumlandırma sorunu, hukuk bilimini, internetle ilgili düzenlemelerin yapıldığı 90 lı yıllardan bu güne kadar meşgul etmektedir. Şöyle ki uzunca bir süre Tele Hizmetler Kanunu'yla medya servisleri anlaşmasının aynı anda geçerli olmasından dolayı internetin tanımı üzerinde bir uzlaşma sağlanamamıştır: Bireysel iletişim aracı mıdır? Radyoyla ilintili midir? Yoksa basın yayın aracıyla mı kıyaslanmalıdır? Bu tarz bir medya aracı alışagelmış düşünce kategorilerimizi ve bununla birlikte hukuki kategorilerimizi de alt üst etmektedir.

Sorunun yeni olması ve hem anayasal hem de hukuksal tanımının yapılmamış olması, bence, bu soruna yaklaşım tarzında şöyle bir eğilimin bulunduğunu saptamayı mümkün kılmaktadır: Ceza kovuşturması organları bahse konu yöntemleri önce bir deneme yoluna gitmektedirler. İstenilen yöntemlerin başvuruları kısa bir süre içerisinde yapılır ve şans eseri fazla ayrıntıya girmeyen bir soruşturma hakimine rastlanıldığında kolayca yetki alınabilir. Bu şekilde ceza muhakemesi hukukundaki, yetki normlarının serbestçe geliştirilmesi esası kullanılmak suretiyle, her türlü takip yöntemi yetki şartına bağlanarak meşrulaştırılabilmektedir. Böylece yapılan hukuki işlemin, kişinin temel hak ve özgürlüklerine her türlü müdahaleyi yasaklayan yasaya uygunluğu, gerektiği gibi denetlenmemektedir.

Bu tarz davranışların gerekçelendirilmesindeki eğilimler, bu alanda farklı olaylar için verilmiş mahkeme kararlarında bulunmaktadır: Ceza Kovuşturması Organlarının, özellikle telekomünikasyonun kontrol edilmesiyle ilgili olan Ceza Muhakemesi Kanunu'nun 100a. maddesinin, uygulanışındaki eğilimi, daha çok telekomünikasyon aracı sayılabilecek her şeyin Ceza Muhakemesi Kanunu'nun 100a. maddesine dayandırarak kontrol edilmesi yönündedir. Anayasanın 10. maddesinde belirtilen, kişinin haberleşme özgürlüğü ve gizliliği karşısında, bu temel hak ve özgürlüklerin

geçerliliğini sağlamak için telekomünikasyon teriminin anlamının geniş kapsamlı ele alınması gerektiği savı da çoğu zaman ileri sürülmektedir. Bu şekilde, bilerek ya da bilmeyerek, bir unsurun kişinin bir temel hak ve özgürlüğünü etkileyecek şekilde geniş kapsamlı ele alınmasının aynı zamanda ceza muhakemesi açısından, bir müdahale yetkisinin de geniş kapsamlı ele alınmasını beraberinde getirdiği çoğu zaman göz ardı edilmektedir. Farklı bir deyişle: Bir koruma tedbirinin, konusu itibariyle bir şekilde temel hak ve özgürlüklerin alanında girdiği gerçeği, bir müdahalenin temel hak ve özgürlüklerinin kısıtlanmasını meşrulaştırabilecek nitelikte olan bir müdahale yetkisini de otomatik olarak beraberinde getirdiği anlamına gelmemektedir. Sonuç itibariyle, telekomünikasyon teriminin geniş kapsamlı ele alınışı anayasanın 10. maddesinde belirtilen bir temel hak ve özgürlüğe müdahale olmasından dolayı, her bir olayın ayrı ayrı gerekçelerinin değerlendirilmesi gerekmektedir.

C. Online Aramayla ilgili Örnek

1. Konu içeriği: Terör olaylarıyla ilgili olduğu varsayılan bir soruşturma işleminde Federal Başsavcı, Federal Mahkeme Soruşturma Hakimine verdiği dilekçeyle zanlının kullanmış olduğu bilgisayarın incelenmesi ve soruşturma organlarınca bazı önlemlerin alınabilmesi için, yani inceleme ve arama amacıyla yapılmış bir bilgisayar programı (Federal Truva Atları=Bundestrojaner), zanlının bilgisayarına göndermek suretiyle, kayıtlı verilerin kopyalanması ve soruşturma organlarına bazı bilgilere ulaşabilmesi için, yetkinin verilmesini talep etmiştir. Federal Mahkeme Soruşturma Hakiminin, Başsavcının bu talebini, bir yıl önce bir başka soruşturma hakiminin karşı yönde bir karar vermiş olmasına rağmen reddetmesi ve böyle bir uygulamaya müsaade etmemesi ve başsavcının yapmış olduğu itirazın dahi değerlendirmemesi üzerine, dosya 3. Ceza Dairesine intikal etmiş ve 3. Ceza Dairesi de aynı yönde karar vererek, bu tarz bir online araştırmaya müsaade etmemiştir.

Bu olayda, şüphesiz bu yönde bir karar de lege lata prensibine göre mutlaka yerindedir. Gizli bir online incelemesi Ceza Muhakemesi Kanunu'nun öngördüğü tarzda bir soruşturma şekli değildir. Çünkü, çok sayıda kanuni düzenlemelerden yola çıkarak, ceza kovuşturma organlarının aleni hareket etmelerini gerektirmektedir. Online incelemede müdahalenin ağırlığının bu kadar yüksek olmasının sebebi, geleneksel incelemelerin aksine sadece belirli bir zaman diliminde sonuç alınabilmesindedir ve aynı zamanda yapılan incelemenin uzunca bir süre devam ettirilebilir olmasındandır. Aynı zamanda online inceleme bir telekomünikasyon incelemesidir. Çünkü bu inceleme ile, öncelikle elektronik ortamda oluşturulmuş içerikler değil; inceleme sırasında sürdürülen iletişim işlemleri incelenmektedir. Elde edilen verilerin ceza kovuşturma organlarına aktarılması, sadece ilgili şahsın internet bağlantısının gerçekleştirdiğinde

mümkün olması bir şeyi deęiřtirmez. Zira, bilgisi alınan tek gerek zamanlı iletiřim, Federal Truva Atları programının devreye girmesiyle elde edilen verilerin kovuřturma organlarına aktarıldığı zamandır.

Federal Mahkemenin kararına göre, böyle bir yetkinin, eřzamanlı devreye giren birbirinden farklı soruřturma yetkilerinin toplamından oluřturulması ya da bu yetkilerin birbirine benzemesinden dolayı, yetki alanın geniřletilmesinin kanuni gerekelere dayandırılması mümkün deęil, aksine bir ceza davasında koruma tedbirlerinin anayasaya uygunluęu aısından aık bir hukuki dayanak gerektirmektedir.

2. Her ne kadar kayıtsız řartsız olarak Federal Mahkemeye hak vermek gerekse ve bu somut olayda olumlu bir sonu alınmış olsa da, bu olayda yukarıda bahsedilen sorunları ortaya koymaktadır: Gerek Cumhuriyet savcısının gerekse bir ka ay önce Federal Yüksek Mahkemenin bir bařka Soruřturma Hakiminin gizli online incelemesini yasal kabul etmesi, hukuki bir güvensizlik ortamı yaratmıştır. Bu durum, ilgili temel hak ve özgürlüklerin doęru sınıflandırılmasını zorlařmaktadır ve yukarıda bahsedilen “denemesi mümkün” anlayışı hem bařsavcılık tarafından gayet sıradan bir iřlemden farksız olarak verilen dilekede hem de soruřturma hakiminin kararı üzerine yapılan itirazda kendisini aıka göstermektedir.

De lege lata prensibi itibariyle bu sorun Federal Yüksek Mahkeme tarafından tatmin edici bir řekilde ortadan kaldırılmıştır ve derinlemesine bir inceleme gerektirmemektedir. Daha ilgin olabilecek durum ise de lege ferenda prensibi itibariyle ortaya ıkabilecek olasılıklar ve nelere dikkat edilmesi gerektiğidir: İlk plandaki yetkisi, adli kolluk deęil, önleyici kolluk olan ve Federal Adalet Bakanı Zypries gibi inatı bir muhalifi bulunan Federal İiřleri Bakanı Schäuble fazla zaman kaybetmeden bu konuyla ilgili kanuni düzenlemelerin yapılması gereklilięini ifade etmiştir. Federal emniyet teřkilatı da aynı talepte bulunmuş. Thüringen Eyalet Temsilcileri Meclisine, gizli online aramanın kanuni düzenlemelerinin yapılmasını talep etmiştir. řu an Federal Mecliste görüřülen ceza Muhakemesi Yasası reformları ierisinde telekomünikasyon aletlerinin gözetimi ve dięer gizli soruřturma yöntemleri konusunda buna benzer bir düzenlemeye yer verilmemesine raęmen, zaman ierisinde bu konuyla ilgili geliřmelerin olmaması kanaatimce kesin deęildir. Kuzey Ren-Vestfalya eyaletinde polisin soruřturma ařamasında bu yönde bir düzenleme mevcut ve hatta bu düzenlemenin Kanuna uygunluęu ile ilgili ilk řikayet bile ibraz edilmiştir.

3. Online aramayla ilgili bir yasal düzenleme, bence yakın bir zamanda yapılacaktır. Bunun Kriminoloji taktięiyle ilgili önemli avantajları bulunmaktadır. Ayrıntıların nasıl düzenleneceęi sorunundan baęımsız olarak bu tür varsayıma dayanan bir düzenleme modern soruřturma yöntemlerinin anayasal aıdan nerede yer alacaęı sorununa iyi bir örnek teřkil etmektedir. Deęiřik temel hak ve özgürlükler söz konusu olmakla birlikte,

bunlardan bazılarının öncelikli olup olmadığı ve eğer öyleyse hangilerinin öncelikli olduğu tartışmalara açıktır.

a) Bir yasal düzenlemenin oluşumunda belki de en ilginç soru, bir gizli online aramanın Anayasanın 13. maddesiyle koruma altına alınmış olan özel yaşam hakkının dokunulmazlığına müdahale sayılıp sayılmayacağı ve sayılırsa ne zaman böyle bir durum söz konusu olduğudur. Anayasanın 13. maddesinin bugünkü haliyle ceza muhakemesi yöntemleriyle ilgili klasik arama ve geniş çaplı dinleme dışında herhangi bir anayasal istisna düzenlenmediğinden, verilen her türlü yetkinin anayasaya aykırılık teşkil etmektedir veya bir anayasa değişikliği gerektirmektedir.

Anayasanın 13. maddesinde düzenlenen, kişinin özel yaşam hakkı ve bunun dokunulmazlığı, şahsın özel yaşam alanında, yani evinde rahatsız edilmemesini gerektirmektedir. Kamu iktidarının, kişinin isteği dışında evine müdahale etmesini yasaklamaktadır. Federal Yüksek mahkemenin vermiş olduğu bir kararla, dinlemek amacıyla evin içerisine çeşitli cihazların yerleştirilmesi, bu genel yasağın içerisine dahil edilmiştir. Böylelikle anayasanın 13. maddesi, sadece devletin izinsiz fiziksel olarak evin içerisinde bulunmasından değil, aynı zamanda bugünkü teknolojik imkanların elverdiği ölçüde, korunan bölgenin maddesel engellerinin aşılmasıyla içeriye her türlü müdahaleden de kişiyi korumaktadır. Eğer evin içerisinin gözetlenmesinde kullanılan teknik aletlerin evin dışında konumlandırılması nedeniyle konutun gözetlemeye karşı korunmayacaksa, 13. maddenin sağladığı temel hakkın sağladığı koruma amacı sonuçsuz kalacaktır.

Buna rağmen geçerli olan ve hatta hakim olan görüş, kanaatimce yerinde olmamakla birlikte, online aramanın Anayasanın 13. maddesinden etkilenmediği yöndedir. Gerekçeleri, temel hak ve özgürlüklerin amacıyla, konut dokunulmazlığı, devleti kişinin evinin dışında bırakmaktadır, buna karşı bilgisayarın dışında bırakmayı öngörmemektedir. Ayrıca bir online arama evin içerisindeki olayları kesintisiz olarak aktarmamaktadır. Fakat bilgisayarın internet bağlantısına geçtiği süre içerisinde, her ne kadar sübjektif bir kabulden bahsetmek mümkün olmazsa da, objektif iletişim şartlarının değişmesi ve aleni konuma geçmesi söz konusudur. Bir ev, odaları itibariyle dış dünyaya kapalı olmasına rağmen, bilgisayar üzerinden dış dünyayla iletişime geçilmektedir ve tersi olarak internet üzerinden bilgisayar dış müdahalelere açık olmaktadır. İnternet bağlantısıyla demek ki evin odalarından bağımsız bir virtuel oda oluşmaktadır. Bu durum, ne zaman ki online “olursanız” evin dokunulmazlığından söz etmek mümkün olmadığı anlamına gelmektedir ve söz konusu virtüel odalar anayasanın 13. maddenin korunması içerisinde dahil değildir.

Buna karşı doğru olan, online aramaya maruz kalan bilgisayarın bir evin içerisinde bulunması halinde, Anayasanın 13. maddesindeki koruma alanı içerisinde olduğunun kabulüdür.

İnternete bağlanmakla objektif iletişim şartlarının dışarıya açık hale geldiği görüşü açıkça dayanaksızdır. Öncelikle virtuel bir açılmanın dikkate alındığı halde, firewall ile korunan virtuel bir odanın varlığı dikkate alınmaması açıklanamamaktadır. Özellikle evin sahibinin haberi olup onun izniyle eve giren şahıslarla evin odaları itibariyle korunmasını yok etmemektedir.

Anayasanın 13. maddesi daha çok hangi bilgilerin bir evin içerisinden alınıp alınamayacağına dair bir yetkiyi de içermektedir. Karşı görüşte olanların aksine bir ev, dış etkilere karşı kapalı bir alan teşkil etmektedir. Bazı durumlarda kişinin evinden ya da evinin dışında bir yerden (örneğin bir İnternet Kafede veya bir Hot Spot'da) internete bağlanması tamamen bir tesadüftür. Ancak bu durumun bir tesadüf olması, anayasal korumaya dahil edilemeyeceği anlamına gelmemektedir. Bu anlamda her halde bir evin içerisinde bulunup bulunmadığınız (ve anayasanın 13. maddesinden kaynaklanan bir müdahale engelini bulunup bulunmadığı) tamamen bir tesadüfe bağlıdır. Taşınabilir ve taşınamaz internet bağlantıları arasındaki ilişkiyle kıyaslanabilir bir durumdur. Kendi ortamının dışında internete bağlanmayı mümkün kılan bir notebook veya laptop kavram olarak bizlere Almanya'da taşınabilir ofis olarak anlaşılmasına rağmen kimse evdeki kazanan sürekli aynı yerde konumlandırılmış evdeki bilgisayarı potansiyel bir taşınabilir yayın aracı olarak anlaşılmamaktadır.

b) Tüm bunların dışında ilk bakışta şaşırtsa da anayasanın 10. maddesinde belirtilen haberleşmenin gizliliğinin korunması, online arama ile her zaman ihlal edilmemektedir. Bir haberleşme işlemi sonucunda oluşan belgelerin özellikle (e-maillerde) haberleşme özgürlüğüne bir müdahale söz konusu olabilir, ancak bu durum sadece haberleşmenin halihazırda devam ettiği süre içerisinde söz konusu olacaktır. Gelecekte yapılacak olan şifreli haberleşme işlemlerinin (örneğin e-mail yazışmalarının veya telefon görüşmelerinin) şifresini kırmak amacıyla yapılacak online arama buna bir istisna olarak kabul edilmektedir, çünkü ileri bir zamanda yapılması planlanan haberleşme gözetimiyle doğrudan ilintilidir. Tabii ki böyle bir ilişkinin kurulması, burada savunulan bir evde bulunan bilgisayarın Anayasanın 13. maddesiyle korunması düşüncesinden çok daha yapaydır.

c) Eğer baştan itibaren haberleşmenin gizliliği esası kabul edilmiyorsa (ki, bu mümkün) burada savunulan görüşün aksine, Anayasanın 13. maddesinin de uygulanamayacağı görülmektedir. Bu durumda geriye sadece kişinin kendini özgürce geliştirme özgürlüğü kalmaktadır. Bu, Federal Anayasa Mahkemesinin nüfus sayımıyla

ilgili olan ve Mahkemenin resmi yayınlarının 65. cildinde yayınlanmış olan kararında, insan onurunun ve kişinin özel yaşam hakkının etkisi olarak ortaya çıkmaktadır.

Bilgisayarda kayıtlı verilerin, belgelerin çoğu bilgisayar kullanıcısının şahsıyla ilgili olduğundan, onların kopyalanması kişinin özgürce kendini geliştirme özgürlüğüne bir müdahale sayılacaktır. Böyle bir müdahalenin hangi durumlarda meşru sayılabileceği hem verilen yetki kuralının yapısına, hem de soruşturmaya konu olan olayın somut şekline bağlıdır; fakat, her şeyden önce aramaya konu belgenin içeriğine bağlıdır. Eğer bilgisayarda kayıtlı belgeler bir günlük niteliği taşıyorsa (ki, bu mümkün), yapılacak işlem, hemen kişinin özel yaşam hakkına bir müdahale şeklini almaktadır ve insan onuruna saldırı niteliği taşıyan bu tarz bir müdahale çok kısıtlı şartlarda mümkündür.

Detaylarla ilgili bu sorun haricinde temel hak ve özgürlüklerle olan bağlantıda daha önemli olan kişinin kendini özgürce geliştirme hakkının genel bir çıkış noktası teşkil etmesidir: Fakat bu temel hak ve özgürlüğün etkilendiğini kabulle yetinir ve kişinin konut özgürlüğüne müdahaleyi yok farz edersek, kanaatimce bu müdahaleyi küçümsemiş olacağız. Kişinin kendi kendini geliştirme hakkı başka konularla ilişkilendirildiği anda, olduğundan fazla önemsenmektedir. Marjinal şekilde kişiliklerin etkilenmesi temel hak ve özgürlüklere bir saldırı olarak nitelendirilmeye çalışılmaktadır. Tren istasyonlarına yerleştirilen güvenlik kameralarıyla yapılan video kayıtları ve gizli olarak yapılan online aramaların kişinin temel hak ve özgürlüklerine müdahalenin şiddeti açısından aynı statüye konması, burada bir ölçütün olmadığını göstermektedir.

D. Üst Sırada Yer Alan Bir Sorun Olarak Kişinin Özel Yaşam Alanının Korunması

Bir online araştırmada kişinin şahsiyetiyle ilgili bilgilerden günlük tarzında yazılara kadar hususlara rastlanması, daha üst boyutta bir soruna işaret etmektedir. Bu sorun sadece online aramada değil her türlü koruma tedbirinde ve hatta modern teknoloji aletlerinin kullanılmadığı her türlü güvenlik kontrollerinde karşımıza çıkmaktadır.

Federal Anayasa Mahkemesi'nin 2004 yılında verdiği ve evin içerisindeki aleni olmayan konuşmaların dinlenmesini yasal kabul ettiği kararında, her türlü suç kovuşturmasında özel yaşamın özünün korunması gerektiğine işaret etmiştir. Kişinin, (günlük kayıtlarının haricinde) güvendiği insanlarla olan haberleşmesinde dahi bu öze bir müdahale olabilir ve bu durumda bir kontrol mümkün olmayacaktır, kontrol edilse de mahkemece değerlendirilemeyecektir. Yukarıda sözü edilen Alman Ceza Muhakemesi Yasası reformunda, alenen yürütülmeyen soruşturma yöntemleri açısından, Federal Anayasa Mahkemesinin işaret etmiş olduğu bu husus değişik

şekillerde ele alınmıştır. Bazı hususların kanunlara uyarlanması güç görünmekte ve şimdiden tartışmalara konu edilmektedir. Bununla ilgili iki örnek vermek gerekirse:

Daha önce bahsetmiş olduğum Kuzey Ren-Vestfalya eyaletinin Anayasayı Koruma Kanununda online incelemenin sınırlarıyla ve veri değerlendirme yasaklarıyla ilgili hiçbir madde bulunmamaktadır. Kuzey Ren-Vestfalya eyaletinin yasama organı bu tarz sınırlamaların sadece evlerin akustik dinlenmesi yoluyla yapılan araştırmalarda geçerli olduğundan yola çıkmaktadır ki, bu tarz bir yaklaşım fazlasıyla naif sayılır.

Diğer taraftan, muhasebeciler ve hekimler gibi meslek gruplarının yararlarını savunan lobiler, belirli meslek grupları açısından ancak özel yaşamın özüne dokunulmasının ispatı durumunda göreceli bir delil yasağı kabul edildiği halde, müdafî, psikolog ve milletvekilleri gibi diğer bazı meslek gruplarında tam bir ispat yasağı kabul edilmesinden şikayet etmektedirler. Bu şikayetler şaşırtıcıdır. Çünkü, belirtilen meslek sahipleri ile onların „müşterileri“ (yani hasta, müvekkil vs.) arasındaki ilişkinin korunma derecesi bugüne kadarki hukuksal durum karşısında her halükarda güçlenmiştir.

E. Sonuç

Verilen bu kısa sürede sadece ana hatlarıyla ve sadece bir örnekle şu günlerde Almanya’da tartışılan konular arasında popüler olan, dijital çağda ceza soruşturma organlarının araştırmalarında özel yaşam hakkının korunmasına dair sorunları derinleştirmek mümkün olmuştur. Burada, ceza soruşturması ile temel hakların korunması arasındaki dengeyi kaybetmemeye yönelik önemli yapısal sorunlar netleşmiştir. “Gizlemeye ihtiyacı olmayanın korkmaya da ihtiyacının olmadığı” anlayışı, toplumun modern iletişim araçlarına, ama aynı zamanda da kamu erkine olan güvenini güçlendirmek açısından kesinlikle yardımcı olmadığı gibi, neredeyse hiç uygun da değildir.

Diğer taraftan karamsar da olmamak gereklidir: Yukarıda belirtilen muhasebeci ve hekimlerin Alman Ceza Muhakemesi Yasası Reformu bağlamında, sahip oldukları dezavantajlarıyla ilgili şikayetlerine ilişkin anektod, Almanya’da ara sıra „yüksek derecede hayıflanıldığını“ göstermektedir. Bazı kaçınılmaz zorluklar, öncelikle modern suçluluk realitesine uygun etkin ceza soruşturmasını dikkate almaksızın, Alman Anayasası vasıtası ile göreceli olarak yüksek bir koruma derecesinin beklenmesi denemesinde ortaya çıkmaktadır. Her yerde tehlike ve devletin suiistimalini gören, her zaman ve her kuralda bir kusur bulacaktır. Bu tür bir güvensizlik ortamında, günlük uygulamada var olan, kara yolları trafiği alanında basit suçların aydınlatılmasında kan alınması biçimindeki bedene müdahalenin gerçekleştirilip gerçekleştirilemeyeceği

sorununun bir kez daha tartışılması gerektiği akla gelmektedir. Sadece gizlice gerçekleştirilen ve belirli bir bölgeyi kapsayan gen incelemeleri ve bu verilerin kullanılması düşünüldüğünde, alınan kan açısından da bir suiistimal potansiyeli bulunmaktadır. Bu türden kan almaların nispeten uzun bir geçmişi olmasına rağmen, istenmeyen bu durumlar, en azından bildiğimiz kadarıyla gerçekleşmemiştir. Temel haklara yönelik müdahalelerin bütün hassaslığına ve canlılığına rağmen, sonuna kadar iyimserliğimizi korumalıyız.