BUNDESPATENTGERICHT

23 W (pat) 27/18

_____

(Aktenzeichen)

Verkündet am
11. Juli 2019
…

B E S C H L U S S

In der Beschwerdesache

betreffend die Patentanmeldung 10 2009 009 276.5

hat der 23. Senat (Technischer Beschwerdesenat) des Bundespatentgerichts auf die mündliche Verhandlung vom 11. Juli 2019 unter Mitwirkung des Richters Dr. Friedrich als Vorsitzenden sowie der Richter Dr. Zebisch, Dr. Himmelmann und Dr. Kapels

beschlossen:

Die Beschwerde wird zurückgewiesen.

ECLI:DE:BPatG:2019:110719B23Wpat27.18.0

G r ü n d e

I.

Die vorliegende Anmeldung mit dem Aktenzeichen 10 2009 009 276.5 und der Bezeichnung „Verfahren zum Missbrauchsschutz von Adressendateien“ wurde am 17. Februar 2009 beim Deutschen Patent- und Markenamt zur Prüfung eingereicht.

Die Prüfungsstelle für Klasse H04L hat im Prüfungsverfahren auf den Stand der Technik gemäß den Druckschriften

D1 US 2006 / 0 106 799 A1 und
D2 US 2008 / 0 168 047 A1

verwiesen und im ersten Prüfungsbescheid vom 2. November 2009 die Patentfähigkeit des Verfahrens nach dem ursprünglichen Anspruch 1 verneint, da das beanspruchte Verfahren dem Fachmann ausgehend von Druckschrift D1 in Verbindung mit Druckschrift D2 nahegelegt werde. Entsprechendes gelte für die Zusatzmerkmale der abhängigen Ansprüche 2 bis 6 und die Gegenstände der selbständigen Ansprüche 7 und 8. Mit Eingabe vom 16. März 2010 hat die Anmelderin einen durch Aufnahme der Merkmale des ursprünglichen Anspruchs 7 präzisierten Anspruch 1 vorgelegt und argumentiert, dass die Druckschriften D1 und D2 das darin beanspruchte Verfahren weder vorwegnehmen noch nahelegen könnten. Dem hat die Prüfungsstelle im zweiten Prüfungsbescheid vom 30. Januar 2013 widersprochen und dargelegt, dass das Verfahren des neuen Anspruchs 1 dem Fachmann ausgehend von Druckschrift D2 in Verbindung mit Druckschrift D1 nahegelegt sei. Die Anmelderin hat daraufhin mit Eingabe vom 28. Mai 2013 einen durch Aufnahme von Merkmalen aus der Beschreibung weiter konkretisierten Anspruch 1 eingereicht, zu dem die Prüfungsstelle mit Ladungszusatz vom 14. Mai 2018 ausgeführt hat, dass auch das darin beanspruchte Verfahren dem Fachmann ausgehend von Druckschrift D2 in Verbindung mit Druckschrift D1

nahegelegt sei. Dementsprechend hat die Prüfungsstelle die Anmeldung zum Ende der am 4. Juli 2018 durchgeführten Anhörung, in der die Anmelderin die Patenterteilung mit den am 28. Mai 2013 eingereichten Ansprüchen beantragt hat, wegen fehlender erfinderischer Tätigkeit zurückgewiesen.

Gegen diesen der Anmelderin mit Anschreiben vom 13. Juli 2018 am 19. Juli 2018 zugestellten Beschluss richtet sich die am 6. August 2018 beim Deutschen Patent- und Markenamt elektronisch eingegangene Beschwerde mit der nachgereichten Beschwerdebegründung vom 25. Juni 2019.

In der mündlichen Verhandlung am 11. Juli 2019 hat die Anmelderin einen neuen Anspruch 1 vorgelegt. Sie beantragt:

1.
den Beschluss der Prüfungsstelle für Klasse H04L des Deutschen Patent- und Markenamts vom 4. Juli 2018 aufzuheben.

2.
Ein Patent zu erteilen mit der Bezeichnung „Verfahren zum Missbrauchsschutz von Adressendateien“, dem Anmeldetag 17. Februar 2009 auf der Grundlage folgender Unterlagen:

- Patentanspruch 1, überreicht in der mündlichen Verhandlung am 11. Juli 2019;
- Patentansprüche 2 bis 8,
- Beschreibungsseiten 1 und 2, jeweils eingegangen im Deutschen Patent- und Markenamt am 29. Mai 2013;
- Beschreibungsseite 2a, als Beschreibungsseite 3 eingegangen im Deutschen Patent- und Markenamt am 18. März 2010;
- Beschreibungsseiten 3 bis 11,
- 4 Blatt Zeichnungen mit Figuren 1 bis 7, jeweils eingegangen im Deutschen Patent- und Markenamt am Anmeldetag.

Der in der mündlichen Verhandlung überreichte Anspruch 1 hat folgenden Wortlaut:

1. Verfahren zum Missbrauchsschutz von Adressendateien (12), die auf maschinenlesbaren Datenträgern (10, 22) gespeichert sind und jeweils Adressdaten für eine Anzahl verschiedener Adressaten enthalten, wobei eine Eingabemaske (30) zur Eingabe einer Adressatenkennung (16) für einen neu in die Adressendatei (12) aufzunehmenden Adressaten bereitgestellt wird, eine Adresse (26) in die Eingabemaske eingegeben wird, und die Adressatenkennung in der Adressendatei (12) auf einem ersten maschinenlesbaren Datenträger (10) gespeichert wird,
   gekennzeichnet, durch die folgenden Schritte:
   auf Seiten eines Dienstanbieters:
   - Unterhalten einer Zielortdatei (20), die für jeden Zielort in einer Auswahl möglicher Zielorte eine Adresse speichert und dieser Adresse eine verschlüsselte Zielortkennung (18) zuordnet, auf einem von dem ersten Datenträger (10) getrennten zweiten maschinenlesbaren Datenträger (22),

   auf Seiten eines Benutzers:
   - Senden der über die Eingabemaske eingegebenen Adresse an die Zielortdatei (20),
   - Empfang einer zu dieser Adresse gehörenden Zielortkennung (18) von der Zielortdatei (20, und
   - Speichern der Zielortkennung anstelle der Adresse in der Adressendatei (12).

Hinsichtlich der abhängigen Ansprüche 2 bis 6 und der nebengeordneten Ansprüche 7 und 8 sowie bezüglich der weiteren Einzelheiten wird auf den Akteninhalt verwiesen.

II.

1. Die form- und fristgerecht eingelegte Beschwerde der Anmelderin ist zulässig. Sie erweist sich aber nach dem Ergebnis der mündlichen Verhandlung als nicht begründet, da dem Fachmann das Verfahren des Anspruchs 1 durch Druckschrift D1 i. V. m. seinem durch Druckschrift D2 belegten Fachwissen nahegelegt wird und folglich gemäß § 1 Abs. 1 PatG i. V. m. § 4 PatG wegen fehlender erfinderischer Tätigkeit nicht patentfähig ist.

Bei dieser Sachlage kann die Zulässigkeit der geltenden Patentansprüche dahingestellt bleiben *(vgl. BGH GRUR 1991, 120-122, insbesondere 121, II.1 - Elastische Bandage)*.

Der zuständige Fachmann ist hier als ein berufserfahrener Hochschulabsolvent der Elektrotechnik oder Informatik, Fachrichtung Datenverarbeitung zu definieren, der sich mit dem sicheren und geschützten Abspeichern personenbezogener Daten befasst.

2. Die Anmeldung betrifft ein Verfahren zum Missbrauchsschutz von auf maschinenlesbaren Datenträgern gespeicherten Adressendateien, wobei eine Eingabemaske zur Eingabe einer Adressatenkennung, bspw. des Namens eines neu in die Adressendatei aufzunehmenden Adressaten bereitgestellt wird, eine Adresse in die Eingabemaske eingegeben und die Adressatenkennung in der Adressendatei auf einem ersten maschinenlesbaren Datenträger gespeichert wird.

Zur Vereinfachung administrativer Vorgänge in der Wirtschaft und öffentlichen Verwaltung wird dort in der Regel auf Adressendateien zurückgegriffen, die elektronisch auf Datenträgern wie DVDs, Festplatten, USB-Speichersticks und dergleichen gespeichert sind. Dies erleichtert nicht nur die Versendung von Rundschreiben oder die Auftragsbearbeitung, sondern gestattet es auch, die Adressen einer Vielzahl von Personen oder Unternehmen zusammen mit Zusatzinformationen in kompakter Form zu speichern und im Bedarfsfall über elektronische Netzwerke

anderen Sachbearbeitern zu übermitteln. Die leichte Kopierbarkeit und Übertragbarkeit der Daten und die Kompaktheit der Datenträger erhöhen jedoch auch die Gefahr des Datendiebstahls und -missbrauchs aufgrund unautorisierten Kopierens der Daten, *vgl. Beschreibungsseite 1 bis 2, erster Absatz.*

Vor diesem Hintergrund liegt der Anmeldung als technisches Problem die Aufgabe zugrunde, ein Verfahren anzugeben, das es erlaubt, Adressendaten besser gegen Missbrauch zu schützen, *vgl. Beschreibungsseite 2, zweiter Absatz.*

Gelöst wird diese Aufgabe durch das Verfahren des Anspruchs 1 und die Softwareprogrammprodukte der Ansprüche 7 und 8.

Das beanspruchte Verfahren ist in der Anmeldung anhand der nachfolgend wiedergegebenen Figuren 1 bis 3 mit zugehöriger Beschreibung auf den Seiten 4 bis 7 erläutert, wobei in Figur 1 die Aufteilung der Datenspeicherung auf zwei maschinenlesbare Datenträger (10, 22) schematisch dargestellt ist und sich die Figuren 2 und 3 auf das Neuaufnahmeverfahren entsprechend Anspruch 1 beziehen.

Demnach erscheint bei der Erstellung eines neuen Datensatzes (14) auf dem Computerbildschirm des Benutzers eine Eingabemaske (30), in deren eines Feld (32) die Adressatenkennung (16), bspw. der Name des neu aufzunehmenden Adressaten eingetragen wird, und in deren anderes Feld (34) die Klaradresse (26) des Adressaten einzugeben ist.

Durch Anklicken des Speichern-Knopfes (36) sendet die Benutzersoftware in einem Schritt S1 die Klaradresse (26) an den Datenträger (22) des Dienstanbieters mit der Zielortdatei (20), wo ein Datensatz (24) generiert wird, der die Klaradresse (26), ggf. GPS-Daten (28) und die korrespondierende verschlüsselte Zielortkennung (18) des neu aufzunehmenden Adressaten umfasst. In Schritt S2 sendet die Zielortdatei (20) die zugehörige Zielortkennung (18) an den Rechner des Benutzers zurück, wo schließlich in Schritt S3 die empfangene Zielortkennung (18) zu-

sammen mit der Adressatenkennung (16) in einem neuen Datensatz (14) in der Adressendatei (12) auf dem Datenträger (10) des Benutzers gespeichert wird.

Fig. 1

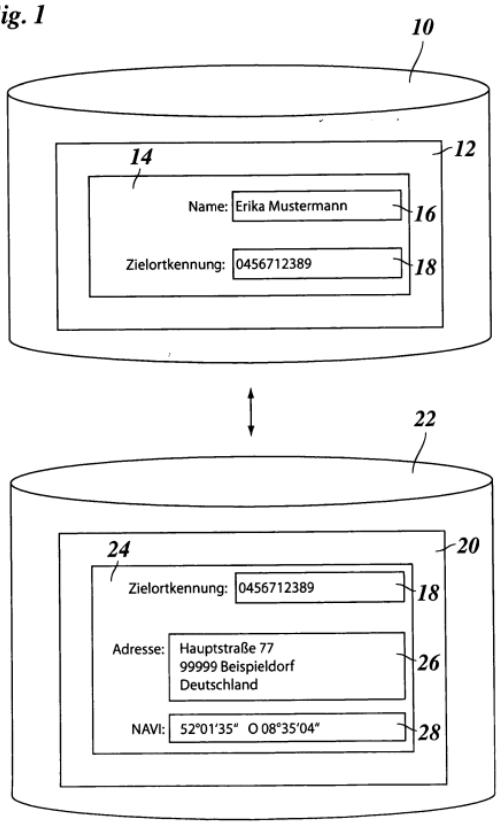


Fig. 2

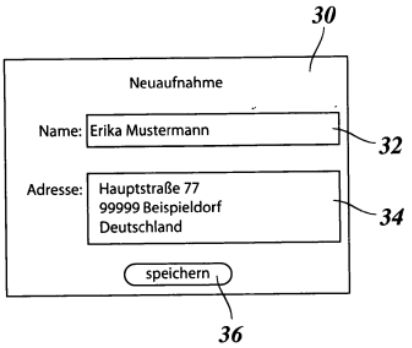
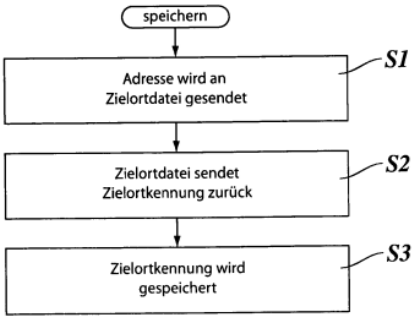


Fig. 3



Das Verfahren des Anspruchs 1 zeichnet sich somit dadurch aus, dass sich zum einen auf dem Datenträger (10) des Benutzers eine Adressendatei (12) befindet, die zwar den Namen (Adressatenkennung 16) des Adressaten umfasst, aber nicht dessen Klaradresse (26), sondern nur die zugehöriger Zielortkennung (18), und dass zum anderen auf dem Datenträger (22) des Dienstanbieters die Zielortdatei (20) gespeichert ist, die zwar die Klaradresse (26) umfasst, aber nicht den Klarnamen (Adressatenkennung 16), sondern nur die verschlüsselte Zielortkennung (18).

Dies bietet den Vorteil, dass bei einem Diebstahl oder unerlaubten Kopieren des Datenträgers (10) des Benutzers kein Zugriff auf die Klaradressen (26) der Adres-

saten möglich ist. Da andererseits der Datenträger (22) des Dienstanbieters leichter zu schützen ist als der/die Datenträger (10) der Benutzer, verringert dies die Gefahr des Datenmissbrauchs, *vgl. Beschreibungsseite 2a, erster Absatz.*

3. Das Verfahren nach Anspruch 1 wird dem Fachmann ausgehend von Druckschrift D1 i. V. m. seinem durch Druckschrift D2 belegten Fachwissen nahegelegt.

Druckschrift D1, vgl. deren Anspruch 1 und die Abs. [0006] und [0007] mit Figuren 1 bis 3, befasst sich ebenso wie die Anmeldung mit der Abspeicherung von Personendaten *(identity data, identity number, first identifier, IDNO)* in einer ersten Datenbank *(first database DB1)*, und, um den Datenmissbrauch zu erschweren, die Abspeicherung von zu schützenden Daten *(sensitive information, drug prescription, DATA)* in einer zweiten Datenbank *(DB2)*, wobei diese Daten mittels einer neu generierten verschlüsselten Kennung *(second identifier, IDENTIFIER)* einander zugeordnet werden.

Dieses Verfahren der Abspeicherung in getrennten Datenbanken ist in Druckschrift D1, vgl. deren nachfolgend wiedergegebenen Figuren 1 bis 3 mit Beschreibung in den Absätzen [0018] bis [0029] und [0037] insbesondere am Beispiel einer ärztlichen Diagnose bzw. der Verschreibung eines rezeptpflichtigen Medikaments *(drug prescription)* erläutert.

Demnach werden im System der Arztpraxis *(health centre system 1)* die Daten in die Eingabemaske *(user interface UI)* eingegeben und über den Telekommunikationsserver *(12)* zu den Datenbanken *(DB1, DB2)* weitergeleitet.

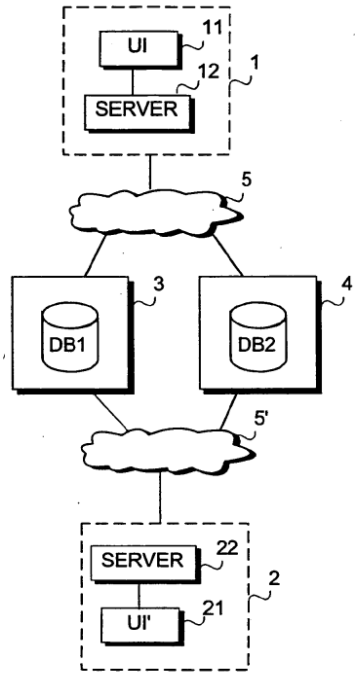


FIG.1

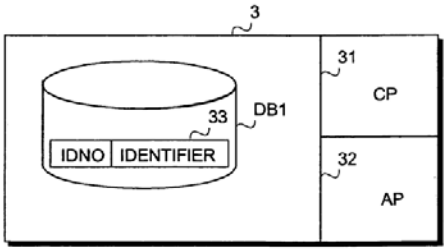


FIG.2

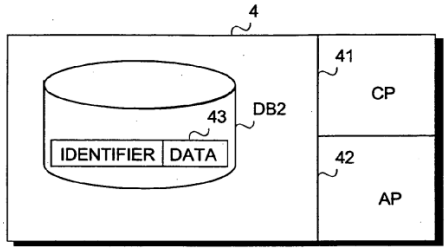


FIG.3

Dabei werden zur Verhinderung des Datenmissbrauchs die individuellen Patientendaten wie die persönliche Krankenversicherungsnummer *(identity number IDNO, first identifier, data identifying an individual)* und eine damit verknüpfte verschlüsselte Kennung *(second identifier, generated identifier)* als Patientendatei *(record 33)* in der ersten Datenbank *(first database, DB1)* gespeichert, wohingegen die Diagnosedaten *(drug prescription, information, DATA)* als zu schützende Information zusammen mit der verschlüsselten Kennung *(second identifier, generated identifier IDENTIFIER)* als Diagnosedatei *(record 43)* in der zweiten Datenbank *(second database, DB2)* gespeichert werden. Über Anwendungs- und Verbindungsmittel *(CP 31, AP 32 CP 41, AP 42)* kann auf die Daten zugegriffen und bei Bedarf die interne ID generiert werden, *vgl. Abs. [0029].*

Das in Druckschrift D1 beschriebene Verfahren bezieht sich somit auf ärztliche Diagnosen *(drug prescription, vgl. Abs. [0006] und [0007])* als zu schützende Daten, während anmeldungsgemäß Adressen zu schützen sind.

Übertragen auf Anspruch 1 entsprechen der *„first identifier“* bzw. die „*identity number IDNO*“ dem Namen des Adressaten (=Adressatenkennung), der „*second*

identifier“ bzw. der *„generated identifier IDENTIFIER“* der verschlüsselten Zielortkennung und die *„sensitive information DATA*“ bzw. *„drug prescription“* der Adresse des Adressaten.

Im Einzelnen offenbart Druckschrift D1 mit den Worten des geltenden Anspruchs 1 ein (Unterschiede zum Anspruch 1 sind durch- bzw. unterstrichen):

Verfahren zum Missbrauchsschutz von ~~Adressen~~Patientendateien

(*patient data / vgl. Abs. [0001] // A method of storing sensitive information / vgl. Anspruch 1)*,

die auf maschinenlesbaren Datenträgern

(interlinked databases / vgl. Abs. [0023] // first database DB1, second database DB2 / vgl. Anspruch 1, Fig. 1)

gespeichert sind und jeweils ~~Adress~~Patientendaten für eine Anzahl verschiedener ~~Adressaten~~ Patienten enthalten

([…] *by storing the individual's identity data in a first database and the sensitive information in a second database […] / vgl. Abs. [0007]*),

wobei eine Eingabemaske

(user interface UI / vgl. Fig. 1 // receiving a storage request / vgl. Anspruch 1)

zur Eingabe einer ~~Adressaten~~Patientenkennung

(first identifier, identity number IDNO / vgl. Anspruch 1, Fig. 2)

für einen neu in die ~~Adressen~~Patientendatei aufzunehmenden ~~Adressaten~~ Patienten bereitgestellt wird, eine ~~Adresse~~ Diagnose

(drug prescription, the information to be stored, DATA / vgl. Abs. [0007], Anspruch 1, Fig. 3)

in die Eingabemaske eingegeben wird

(vgl. Abs. [0020]),

und die ~~Adressaten~~Patientenkennung

(first identifier, IDNO)

in der ~~Adressen~~Patientendatei

(records 33 / vgl. Fig. 2)

auf einem ersten maschinenlesbaren Datenträger

(first database DB1 / vgl. Anspruch 1 und Fig. 2)

gespeichert wird, **gekennzeichnet**, durch die folgenden Schritte:

auf Seiten eines Dienstanbieters:

- Unterhalten einer ~~Zielort~~Diagnosedatei *(records 43 / vgl. Fig. 3)*, die für jede~~n~~ ~~Zielort~~Diagnose *(drug prescription, the information to be stored, DATA / vgl. Abs. [0007], Anspruch 1, Fig. 3*) in einer Auswahl möglicher ~~Zielorte~~ Diagnosen eine ~~Adresse~~ Diagnose speichert und dieser ~~Adresse~~ Diagnose eine verschlüsselte ~~Zielort~~kennung *(second identifier, IDENTIFIER / vgl. Anspruch 1 und Fig. 3)* zuordnet *(The database DB2 comprising prescriptions includes records 43, wherein all drug prescriptions and any other data associated with the identifier are connected to a generated identifier IDENTIFIER in the exemplary embodiment / vgl. Abs. [0037])*, auf einem von dem ersten Datenträger *(first database, DB1)* getrennten zweiten maschinenlesbaren Datenträger *(second database, DB2)*,

auf Seiten eines Benutzers *(user interface UI / vgl. Fig. 1)*:

- Senden der über die Eingabemaske eingegebenen ~~Adresse~~ Diagnose (*drug prescription, the information to be stored, DATA*) an die ~~Zielort~~Diagnosedatei *(record 43)*,
- Empfang einer zu ~~dieser Adresse~~ der Patientenkennung gehörenden ~~Zielort~~kennung *(second identifier / vgl. Anspruch 1)* von der ~~Zielort~~Patientendatei *(vgl. Abs. [0029])*, und
- Speichern der ~~Zielort~~kennung anstelle der ~~Adresse~~ Diagnose in der ~~Adressen~~Patientendatei *(33)*.

Das Verfahren nach Anspruch 1 unterscheidet sich somit dahingehend von dem in Druckschrift D1 offenbarten Verfahren, dass

a) anspruchsgemäß in der einen Datenbank die Adressendatei mit den Adressatenkennungen, bspw. den Namen der Adressaten, und in der anderen Datenbank die Zielortdatei mit den Adressen der Adressaten abgespeichert werden, wohingegen nach der Lehre von Druckschrift D1 in der einen Datenbank die Patientendatei mit den Patientenkennungen, bspw. der individuellen Krankenversicherungsnummer, und in der anderen Datenbank die Diagnosedatei mit den ärztlichen Verschreibungen und Diagnosen abgespeichert werden, und dass

b) anspruchsgemäß die auf Seiten eines Benutzers von der Zielortdatei empfangene verschlüsselte Kennung als Zielortkennung zu einer jeweiligen Adresse gehört, wohingegen nach der Lehre von Druckschrift D1 die verschlüsselte Kennung zu einer jeweiligen Patientenkennung gehört und auf Seiten eines Benutzers von der Patientendatei empfangen wird.

Diese beiden Merkmale können aber keine erfinderische Tätigkeit des Fachmanns begründen.

Denn die Lehre von D1 beschränkt sich nicht auf den Schutz von Diagnosedaten, sondern bezieht sich in allgemeiner Weise auf den Schutz persönlicher Daten, worunter der Fachmann insbesondere auch den Schutz persönlicher Adressdaten versteht (vgl. Abs. [0001]: *„The invention relates to storing sensitive information concerning an individual […]“* oder auch Anspruch 1: „*A method of storing sensitive information in a system comprising two databases […]*“.). Zudem verweist Druckschrift D1 in Abs. [0017], letzter Satz, auf die Möglichkeit, das beschriebene Verfahren zur Speicherung von Rechnungs- und Kaufinformationen im Internethandel einzusetzen *(The invention is also applicable for instance to storing billing and/or purchase information in Internet commerce.)*, was dem Fachmann ebenfalls den Hinweis gibt, die Lehre der D1 für die getrennte Speicherung von Namen und Adressen einzusetzen, insbesondere, da, wie durch Druckschrift D2 belegt, die Geheimhaltung von Adressen zur Gewährleistung der Privatsphäre des Käufers

im Internethandel ein übliches und bekanntes Verfahren darstellt, vgl. die Abs. [0001] bis [0007], Anspruch 1 und Fig. 9 mit Abs. [0042] der Druckschrift D2.

In der einen Datenbank die Adresse als zu schützende persönliche Information abzuspeichern und in der anderen Datenbank den Adressatennamen, ergibt sich somit für den Fachmann in naheliegender Weise aus obigen Fundstellen von Druckschrift D1 i. V. m. seinem durch Druckschrift D2 belegten Fachwissen.

Gleiches gilt für das Merkmal, dass die verschlüsselte Kennung zu einer jeweiligen Adresse gehört und der Benutzer die Kennung von der Datenbank mit den Adressen der Adressaten empfängt.

Denn beim Einsatz des in Druckschrift D1 beschriebenen Verfahrens zur Speicherung von Rechnungs- und Kaufinformationen im Internethandel gemäß dem dortigen Abs. [0017] steht im Vordergrund, die Kaufinformation einer eindeutigen Lieferadresse zuordnen zu können. Dies kann aber nur dann gewährleistet werden, wenn die verschlüsselte Kennung zur Adresse gehört, da ansonsten bei Namensgleichheit unterschiedlicher Käufer oder beim Vorhandensein mehrerer Adressen desselben Käufers keine eindeutige Zuordnung möglich wäre. Aufgrund dieser offensichtlichen Fehlerquelle wird der Fachmann ausgehend von Druckschrift D1 das dort beschriebene Verfahren entsprechend anpassen, so dass die verschlüsselte Kennung nicht zum Namen, sondern zur Adresse des Adressaten gehört und durch den Benutzer von der Datenbank mit den Adressen der Adressaten empfangen wird, wie es ja auch in Druckschrift D2 beschrieben ist, vgl. deren Anspruch 1.

Das Verfahren des Anspruchs 1 ergibt sich somit für den Fachmann in naheliegender Weise aus Druckschrift D1 i. V. m. seinem durch Druckschrift D2 belegten Fachwissen und ist folglich wegen fehlender erfinderischer Tätigkeit auch nicht patentfähig.

4. Es kann dahingestellt bleiben, ob die Gegenstände der formal nebengeordneten Ansprüche 7 und 8 sowie die Verfahren der abhängigen Ansprüche patentfähig sind, denn wegen der Antragsbindung im Patenterteilungsverfahren fallen mit dem Patentanspruch 1 auch die mittelbar oder unmittelbar auf die selbständigen Patentansprüche rückbezogenen Unteransprüche *(vgl. BGH GRUR 2007, 862, 863 Tz. 18 – Informationsübermittlungsverfahren II m. w. N.)*.

5. Bei dieser Sachlage war die Beschwerde der Anmelderin zurückzuweisen.

III.

R e c h t s m i t t e l b e l e h r u n g

Gegen diesen Beschluss steht der Anmelderin - vorbehaltlich des Vorliegens der weiteren Rechtsmittelvoraussetzungen, insbesondere einer Beschwer - das Rechtsmittel der Rechtsbeschwerde zu. Da der Senat die Rechtsbeschwerde nicht zugelassen hat, ist sie nur statthaft, wenn einer der nachfolgenden Verfahrensmängel gerügt wird, nämlich

1. dass das beschließende Gericht nicht vorschriftsmäßig besetzt war,
2. dass bei dem Beschluss ein Richter mitgewirkt hat, der von der Ausübung des Richteramtes kraft Gesetzes ausgeschlossen oder wegen Besorgnis der Befangenheit mit Erfolg abgelehnt war,
3. dass einem Beteiligten das rechtliche Gehör versagt war,
4. dass ein Beteiligter im Verfahren nicht nach Vorschrift des Gesetzes vertreten war, sofern er nicht der Führung des Verfahrens ausdrücklich oder stillschweigend zugestimmt hat,

5. dass der Beschluss aufgrund einer mündlichen Verhandlung ergangen ist, bei der die Vorschriften über die Öffentlichkeit des Verfahrens verletzt worden sind, oder
6. dass der Beschluss nicht mit Gründen versehen ist.

Die Rechtsbeschwerde ist **innerhalb eines Monats** nach Zustellung des Beschlusses

schriftlich durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten beim Bundesgerichtshof, Herrenstr. 45a, 76133 Karlsruhe, einzureichen oder

durch einen beim Bundesgerichtshof zugelassenen Rechtsanwalt als Bevollmächtigten in elektronischer Form. Zur Entgegennahme elektronischer Dokumente ist die elektronische Poststelle des Bundesgerichtshofs bestimmt. Die elektronische Poststelle des Bundesgerichtshofs ist über die auf der Internetseite **www.bundesgerichtshof.de/erv.html** bezeichneten Kommunikationswege erreichbar. Die Einreichung erfolgt durch die Übertragung des elektronischen Dokuments in die elektronische Poststelle. Elektronische Dokumente sind mit einer qualifizierten elektronischen Signatur oder mit einer fortgeschrittenen elektronischen Signatur zu versehen.

Dr. Friedrich Dr. Zebisch Dr. Himmelmann Dr. Kapels

prö