Piratenpartei Deutschland

Klarmachen zum Ändern!

I

Piratenpartei Deutschland -Postfach 02 46 69 -10128 Berlin

Max Mustermann
Musterstraße 1
12345 Musterstadt

7. Oktober 2009

Verpflichtung zur Wahrung des Datenschutzes

Hallo Pirat,

Du wirst hiermit auf den Datenschutz und auf einen verantwortungsvollen Umgang mit den Dir anvertrauten persönlichen Daten und Informationen der Piraten verpflichtet.

Im Folgenden werden unter Mitgliederdaten die Daten und Dokumente verstanden, die für die Verwaltung der Mitglieder erhoben und erstellt werden. Außerdem fallen hierunter alle datenschutzrelevanten Informationen über Piraten, Interessenten und anderen Personen, die Dir im Zuge Deiner Tätigkeiten bekannt werden.

Diese Datenschutzerklärung gliedert sich in:

I Verpflichtung auf den Datenschutz und das Datengeheimnis
II Hinweis zur Sorgfaltspflicht
III Anhang mit den relevanten Gesetzestexten

II Verpflichtung auf den Datenschutz und das Datengeheimnis

Pirat: [Vorname] [Name], geboren [Geb. Dat.] in der Funktion [Helfer der Geschäftstelle]

wird hiermit auf die Wahrung des Datengeheimnisses nach § 5 Bundesdatenschutzgesetz (BDSG) verpflichtet. Diese Verpflichtung besteht auch nach der Beendigung meiner Tätigkeit oder Mitgliedschaft bei der Piratenpartei Deutschland fort.

Ich verpflichte mich,

- zum Schutz der Daten im Rahmen der übertragenen Aufgabe die notwendige Sorgfalt anzuwenden und festgestellte Mängel umgehend dem Vorstand zu melden. Sollte dieser keine Abhilfe schaffen, werde ich selbständig umgehend den Datenschutzbeauftragten und erneut den Vorstand der Piratenpartei Deutschland informieren.
- Passwörter nicht an Dritte weiterzugeben.
- Mitgliederdaten nicht unzulässig zu ändern
- Mitgliederdaten angemessen gegen unbefugten Zugriff zu schützen, so wie dies in den Hinweisen unter Abschnitt II oder in der jeweils aktuellen Fassung beschrieben ist.
- auch nach der Beendigung meiner Tätigkeit oder Mitgliedschaft bei der Piratenpartei Deutschland keine personenbezogenen Daten unbefugt zu verarbeiten oder zu nutzen.
- auch nach dem Ende meiner Tätigkeit oder Mitgliedschaft bei der Piratenpartei Deutschland weder mündlich noch schriftlich Informationen über die Mitgliederdaten an Unbefugte weiterzugeben.

Mir ist bekannt, dass ich keinerlei Informationen und Daten, die mir bei der Ausführung meiner Tätigkeit bekannt werden, an Dritte weitergeben darf. Der Vorstand der Piratenpartei Deutschland kann hierzu im Rahmen der gesetzlichen Möglichkeiten eine Ausnahme zulassen und wird mir dies ausdrücklich in geeigneter und nachvollziehbarer Form für den Einzelfall erklären.

Mir ist auch bewusst, dass die Piratenpartei Deutschland und die betroffenen Personen bei Verstößen gegen die vorgenannten Pflichten zum Daten- und Geheimnisschutz zur sofortigen Geltendmachung von Schadensersatzansprüchen berechtigt sind.

Verstöße gegen den Datenschutz oder strafbare Handlungen gemäß dem Anhang III können mit Geldbußen oder Geld- oder Freiheitsstrafen geahndet werden. Die Bußgeld- und Strafvorschriften des §§ 43 und 44 BDSG (Anlage) habe ich zur Kenntnis genom-

men. Ich verpflichte mich, sämtliche Handlungen zu unterlassen, welche zur Verwirklichung dieser Straftat führen können.

Fragen zum Datenschutz beantwortet Ihnen die Bundesgeschäftsstelle bzw. der Generalsekretär der Piratenpartei Deutschland. Diese werden bei neuen Fragestellungen den Datenschutzbeauftragten der Bundesgeschäftsstelle zur Klärung des Sachverhaltes einschalten. Da der Datenschutzbeauftragte ein professioneller Dienstleister ist und diese Dienstleistung zu Sonderkonditionen erbringt, ist dieser Weg so einzuhalten und außer in dringenden Fällen von einer direkten Kontaktaufnahme abzusehen.

Ich bestätige durch meine Unterschrift, dass ich diese Datenschutzerklärung gelesen und verstanden habe.

Der Verpflichtete

_____

Ort, Datum Unterschrift

Für die Piratenpartei Deutschland

_____

III konkrete Verpflichtungen zur Sorgfaltspflicht

a) Vorbemerkung

Die folgenden Anweisungen im Rahmen der Verpflichtungserklärung sind wesentlich konkreter als die allgemeinen Hinweise zur Datenschutzerklärung.

Diese können sich daher je nach dem Stand der aktuellen politischen und technischen Entwicklungen im Laufe der Zeit ändern. Änderungen dieser Hinweise wird Dir der Vorstand rechtzeitig in geeigneter Form mitteilen. Solltest Du unter diesen Voraussetzungen nicht mehr zur Verfügung stehen, teile dies dem Vorstand bitte umgehend in geeigneter, nachweisbarer Form mit. Du kannst Deine Aufgaben entsprechend dieser Datenschutzerklärung dann an den vom Vorstand zu benennen Nachfolger übergeben. Bis dahin bist Du von Deinen Aufgaben entbunden.

b) Verpflichtung

Ich verpflichte mich

- die Mitgliederdaten auf Datenträgern und Rechnern zu verschlüsseln. Bei Bedarf fordere ich eine Einweisung an.
- Datenträger mit Dateien, die unverschlüsselte Mitgliederdaten beinhalten, bei Nichtgebrauch zum Schutz vor Diebstahl unter Verschluss zu halten.
- den Rechner zu sperren, wenn ich mich vom Rechner entferne und unbefugte Dritte Zugriff auf diesen Rechner haben und die Daten entschlüsselt vorliegen.
- den Bildschirm während der Arbeit an Mitgliederdaten nicht von unbefugten Dritten einsehen zu lassen.
- Mitgliederdaten nur verschlüsselt zu transportieren.
- nicht mehr benötigte unverschlüsselt vorliegende Mitgliederdaten umgehend sicher zu löschen. Bei Bedarf fordere ich eine Einweisung an.
- eine sinnvolle Sicherung des Mitgliederdaten verarbeitenden informationstechnischen Systems gegen äußere Zugriffs- und Manipulationsversuche vorzunehmen.

c) Schutz des informationsverarbeitenden Systems

Ich verpflichte mich ferner

- Vom Hersteller oder Distributor offiziell angebotene Sicherheitsupdates der auf dem Mitgliederdaten verarbeitenden System vorhandenen Software regelmäßig zu installieren. Hierbei kann ich mich von den automatisch verbreiteten Sicherheitsupdates unterstützen lassen.
- Den Rechner mit einer Firewall schützen, wenn dieser lokal oder mit dem Internet vernetzt ist.
- Eine wirksame Antivirensoftware zu installieren und auf dem neuesten Stand zu halten (Aktualisierung mindestens täglich), wenn dies vom Hersteller empfohlen wird.
- Die Arbeit mit Mitgliederdaten an Rechnern strikt zu unterlassen, deren Integrität ich nicht beurteilen kann. Dies ist insbesondere bei öffentlichen Internetzugängen (Internetcafés) der Fall, da hier auch beim Booten von einer sauberen CD//DVD nicht ausgeschlossen werden kann, dass die Daten und die Dateneingaben mit gelesen werden.
- Wenn ich nicht einschätzen kann, ob ein informationstechnisches System kompromittiert ist oder nicht, dieses vor dem Arbeiten mit Mitgliedsdaten sinnvoll auf seine Integrität prüfen, etwa durch den Einsatz von geeigneten Antivirus- und Antimalwareprogrammen. Idealer Weise sollten diese von einem sauberen System gestartet werden. Dies wäre etwa beim Booten einer Live-CD oder DVD wie etwa Knoppicilin der Fall. Bei Fragen hierzu fordere ich eine Einweisung an.
- Die verschlüsselten Datenträger sowie falls notwendig das BIOS und das Betriebssystem muss ich mit sicheren Passwörtern schützen. Als sichere Passwörter gelten nach dem gegenwärtigen Stand solche Passwörter, die mindestens 8 Stellen lang sind und so weit technisch möglich Groß- und Kleinbuchstaben sowie Ziffern und/oder Sonderzeichen enthalten.

d) Administratorrechte

Das Arbeiten mit Administratorrechten sollte vermieden werden. Unter Linux ist dies in der Regel kein Problem, da hier seit Jahren eine sehr strikte Trennung der Funktion „Anwender“ und „Administrator“ vorgenommen wird.

Für Windows-Anwender sind jedoch folgende Hinweise zu Administratorrechten angebracht:

Unter Windows besteht die Problematik, das bestimmte, nicht korrekt programmierte Anwendungen oder Spiele nur als Administrator gestartet werden können.

Hierfür kann man mit einem Rechtsklick auf diese Anwendung diese als Administrator starten. Dazu muss beim verwendeten Administratoraccount in den Ordneroptionen „in einem eigenen Prozess starten“ aktiviert sein.

Keinesfalls darf man Tools einsetzen, die nur dem Browser niedrigere Rechte zuweisen und selbst als Administrator angemeldet sein. Dies zerstört die Sicherheitssystematik von Windows und wird vom Hersteller und von Sicherheitsexperten als große Sicherheitslücke bezeichnet. Auch darf man sich nicht auf die User Account Control von Windows Vista verlassen.

Sind Arbeiten unter echten Administratorrrechten notwendig, sollte man nur auf Seiten anerkannter Anbieter surfen, um Updates und ähnliches zu besorgen. Eine sehr bequeme Lösung für vorübergehende Administratorsessions unter dem eigenen Usernamen ist „Machmichadmin“, das von der c't angeboten wird.

e) Wahl des Betriebssystems, Wahl des Rechners

Das Arbeiten mit Mitgliederdaten der Piratenpartei Deutschland ist mir an Rechnern, deren Betriebssysteme nicht mehr mit sicherheitsrelevanten Updates versorgt werden oder die über keine echte Benutzersteuerung verfügen oder deren Verschlüsselungsmethode als kompromittiert gilt, strikt untersagt. Hierunter fallen Stand 07/2008 unter anderem alle Windows-Betriebssysteme vor Windows XP, aber auch diverse nicht mehr unterstützte Linux-Distributionen und OS2.

Zwar setzt sich die Piratenpartei Deutschland für den freien Zugriff auf Software, Bildung und Informationen ein, jedoch sind nicht lizensierte Windowskopien zu einem hohen Anteil mit Viren und Schadsoftware verseucht und erhalten in vielen Fällen keine Sicherheitsupdates mehr.

Aus diesem Grunde ist mir die Arbeit mit Mitgliederdaten an Rechnern mit nicht lizensier-

ten Windowskopien oder einem sonstigen Betriebssystem, für das mir keine Lizenz eingeräumt wurde, ebenfalls strikt untersagt.

Hierunter fallen selbstverständlich nicht sogenannte „freie“ Betriebssysteme, die kostenlos eingesetzt werden können und für die eine generelle Nutzungslizenz im Rahmen der Open Source-Lizenzierung eingeräumt wurde.

Liegt auf meinem Rechner kein geeignetes Betriebssystem vor, habe ich folgende Alternativen:

- Der Rechner (keine virtuelle Maschine) kann zum Bearbeiten von Mitgliederdaten mit einer sogenannten Live-CD/DVD gestartet werden. Dabei muss man jedoch in regelmäßigen Abständen eine aktuelle Version einer solchen Live-CD erstellen und einsetzen. Zwar können hier die Programme nicht auf dem Datenträger befallen werden. Sicherheitslücken im laufenden System sind jedoch nicht auszuschließen.

- Man kann den Rechner von einer aktuellen Linux-Installations-CD starten und ein Multi-Bootsystem in separaten Partitionen aufsetzen. Dabei ist zu beachten, dass die Daten verschlüsselt abzulegen sind, damit trotz des späteren Startens eines möglicherweise kompromittierten Systems keinesfalls ein Zugriff auf die datenschutzrelevanten Informationen möglich ist.

IV Rechtliche Rahmenbedingungen

- Bundesdatenschutzgesetz §§ 5, 43, 44
- Telekommunikationsgesetz § 88
- Strafgesetzbuch §§ 202, 202a, 202b, 202c, 206, 303a, 303b
- Urteil des BverfG zur sogenannten Onlinedurchsuchung

a) Bundesdatenschutzgesetz (BDSG)

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder

6. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 2 Satz 3 die in § 40 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfundzwanzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu zweihundertfünfzigtausend Euro geahndet werden.

§ 44 Strafvorschriften

(4) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

b) Telekommunikationsgesetz (TKG)

§ 88 Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. 2Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

c) Strafgesetzbuch (StGB)

§ 202 Verletzung des Briefgeheimnisses

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder

2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 149 Abs. 2 und 3 gilt entsprechend.

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,

2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder

3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,

2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,

3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

a) Onlinedurchsuchung

Aus dem Leitsatz zur Onlinedurchsuchung:

„5. Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. Die Maßnahme kann schon dann gerechtfertigt sein, wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen.“

BVerfG, 1 BvR 370/07 vom 27.2.2008

Es erübrigt sich jeder Kommentar dazu, dass derartige Handlungsweisen oder mögliche tatbestandliche Erfolge mit dem Parteiprogramm und den Grundsätzen der Piratenpartei Deutschland absolut unvereinbar sind. Die Folgen einer solchen Handlungsweise durch einen mit offiziellen Aufgaben betrauten Piraten wären klar:

Mit Billigung des BVerfG könnten sämtliche informationstechnischen Systeme der Piratenpartei Deutschlands und Eure eigenen infiltriert und überwacht werden.