

PHÄNOMENE DURCH ÜBERWACHUNG



Zusammenfassende Übersicht von identifizierten
Phänomenen die durch Überwachung auftreten.

(Hg.) Stop Orwell 2020

Impressum:

„Phänomene durch Überwachung“ hg. Stop Orwell 2020, Berlin, Juni 2015

Webseite: www.stop-orwell2020.org

Email: info@stop-orwell2020.org



Dieses Werk von stop-orwell2020.org ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.

Inhaltsverzeichnis

Vorwort.....	4
Phänomene durch Überwachung.....	5
CCTV - Closing Circuit TV (geschlossene Kameraüberwachung).....	5
SNMAS - Social Networking, Monitorin and Analysis systems (Soziale Netzwerke, Kontroll- und Analysesysteme).....	5
FT - Financial Tracking (Finanzverfolgung).....	6
PT - Positioning and Tracking Technologies (Ortsbestimmung- und Verfolgungstechnologien).....	6
DMSM - Data Mining, Data Storage Data Matching (Datenbeurteilung, Datenvorräte, Datenvergleich).....	7

Diese Publikation von Stop-Orwell 2020 basiert auf der Quelle von:

RESPECT - Rules, Expectations and Security through

Privacy-Enhanced Convenient Technologies

(G.A. 285582)

WP13 - Social Costs of Surveillance

LSC - Laboratorio di Scienze della Cittadinanza

(IV/2013)

Vorwort

Überwachung durchdringt unser Leben und unsere Umwelt. Man kann sie weder greifen, riechen noch schmecken. Vielleicht sind gerade deshalb die Phänomene und die Auswirkungen die Überwachung auf Menschen hat, selten Bestandteil öffentlicher Diskussionen. Anhand der folgenden Auflistung wollen wir von Stop Orwell 2020 einen Beitrag dazu leisten, nicht nur auf das Vorhandensein von Überwachungsmaßnahmen hinzuweisen, sondern auch anhand konkreter Überlegungen darstellen, welche negativen Auswirkungen, Überwachung für einen einzelnen Menschen oder für ganze Gruppe haben kann.

In den Vorüberlegungen sind fünf verschiedene Grundmuster und -arten der Überwachung festgestellt worden. Sie unterscheiden sich zum Teil erheblich hinsichtlich ihrer Zielstellung und technischen Umsetzung. Sie unterscheiden sich nicht zwischen staatlichen oder privaten Überwachungsvorgängen.

1. CCTV - Closing Circuit TV (geschlossene Kameraüberwachung)
2. SNMAS - Social Networking, Monitorin and Analysis systems (Soziale Netzwerke, Kontroll- und Analysesysteme)
3. FT - Financial Tracking (Finanzverfolgung)
4. PT - Positioning and Tracking Technologies (Ortsbestimmung- und Verfolgungstechnologien)
5. DMSM - Data Mining, Data Storage, Data Matching (Datenbeurteilung, Datenvorräte, Datenvergleich)

Es gibt sicherlich noch andere Arten und Formen der Überwachung, diese Publikation hat diese fünf, als Basisstock verwendet.

Eine Interpretation der aufgeführten Effekte ist nicht Bestandteil dieser Veröffentlichung. Wir wünschen uns eine allgemeine und breit geführte Diskussion in der Gesellschaft über die Auswirkungen von Überwachung. Dabei erhoffen wir uns insbesondere, dass Überwachung als politisches Instrument deutlich verringert wird.

Phänomene durch Überwachung

CCTV - Closing Circuit TV (geschlossene Kameraüberwachung)

1. Stigmatisierung von spezifischen sozialen Gruppen
2. Rassistische Erfassung und Zerstörung von Vertrauensbeziehungen zu lokalen Communities
3. Negative psychologische Effekte durch Routinearbeit bei CCTV
4. Macht und Verfügungsgewalt auch in automatisierten Systemen der Bediener
5. Vorbeugender Rauswurf von „unerwünschten“ Gruppierungen in sicheren Städtischen Bereichen
6. Datenschutzrisiken im physischen Raum, begrenzen die Bewegungsfreiheit.
7. Unbegründetes und unangemessenes „Suchen und Beschlagnahmen“
8. Erpressung und Bereicherung aus persönlichen Gründen.
9. Bedrohung der freien Meinungsäußerung
10. Video-Voyeurismus und räumliche Vermännlichung
11. Identifikationsfehler durch die „Effektivität“ der automatisierten Technologie
12. Verletzung der Privatsphäre in der Überwachung
13. Repressionen und Sanktionen bei politischen Dissens
14. Verlust des Glauben und Vertrauen in die Polizei
15. Die Polizei verliert ihre Legitimation in den Augen der Öffentlichkeit.
16. Aus eigenen Gutdünken Bruch des Datenschutz in Beziehung zwischen unterschiedlichen Beteiligten. (Öffentlich, Privat, Non-Profit)
17. Verlust des Glauben und Vertrauen in Institutionen
18. Schädliche Effekte auf soziale Beziehungen in Schulen

SNMAS - Social Networking, Monitorin and Analysis systems (Soziale Netzwerke, Kontroll- und Analysesysteme)

19. Beeinträchtigung des privaten Lebens des einzelnen
20. Gefahren der Anonymität in sozialen Netzwerken
21. Widerstände gegen neue intelligente Technologien
22. Unterdrückung des politischen Einwands
23. Selbstzensur im privaten online-Umgang und Veränderungen der Beiträge in Diskussionsforen

24. Ökonomischer und sozialer Schaden hervorgerufen durch abschreckende Wirkung
25. Mögliche Verletzungen von dem Recht auf Verteidigung
26. Unautorisierte Form der Beeinflussung und Kontrolle der politischen Meinungen
27. Gegenseitige Steigerung der Überwachung
28. Erzeugung von aufgebauschter Form von Panik
29. Ermittlungsfehler und Gefahren für verdeckte Ermittler
30. Repressionen bei politischen Widerspruch und soziale Diskriminierung
31. Der Export von Spionagetechnologien für den illegalen Gebrauch von autoritären Regimen
32. Gefahren des ungehinderten freien Ausdrucks im Cyberspace für ethische Minderheiten und religiöse Gruppen
33. Untergrabung der nationalen Souveränität

FT - Financial Tracking (Finanzverfolgung)

34. Unfaire Zielsetzung, Ausschliessung und Diskrimination
35. Verlust des Vertrauen in Banken
36. Schaden des bürgerlichen Ansehens und ökonomischen Aktivitäten
37. Stigmatisierung von Lebensentwürfen
38. Stigmatisierung von Unterstützungszahlungen
39. Finanzielle Beschränkungen haben Auswirkungen auf das tägliche Leben von Bürger
40. Finanz-Identitätsdiebstahl und Auswirkungen auf die Ökonomie und juristischer Schaden.
41. Stress und emotionale Belastung bei Menschen.
42. Missbrauch von Datenbeständen durch Beamte.
43. Ausweichende Reaktionen und Vermeidungsaktivitäten

PT - Positioning and Tracking Technologies (Ortsbestimmung- und Verfolgungstechnologien)

44. Abstraktion der Körper aus ihren Kontext
45. Entmenschlichung und elektronische Vorherrschaft
46. Erosion der bürgerlichen Freiheiten
47. Disipation (Zerstreuung) von Vertrauen und Aufkommen von „gesellschaftlichen teuren“ Stress
48. Fehler bei der Identifikation
49. Belästigungen und Stalking

50. Unbefugter Zugang zu Personendaten, wegen „Überwachungsmissionen“
51. Das Ausbreiten von gegenseitiger Verdächtigung
52. Kontraproduktive Effekte bei Untersuchungen
53. Bruch von lokalen Datenschutzrichtlinien
54. Behinderung von Technologien für die es keine sozialen Notwendigkeiten gibt.
55. Identitätsdiebe auf Grund von Schwachstellen bei RFID-Technologien
56. Anwachsen von nebensächlichen Indizien und falschen Beurteilungen
57. Schaden an politischen und demokratischen Leben
58. Reduzierung der Gesellschaft auf „Innovative“ Potentiale
59. Risiko für Personen in heiklen Positionen
60. Mögliche Datenmanipulation

DMSM - Data Mining, Data Storage Data Matching (Datenbeurteilung, Datenvorräte, Datenvergleich)

61. Hinderungsgründe in der Mobilität bestimmter Gruppierungen
62. Neue Formen von digitaler Kluft
63. Bruch des Versprechens auf Vertraulichkeit
64. Verschwinden der Möglichkeit auf Anonymität
65. Erzeugung von gefälschten „virtuellen Kopien“
66. Geo-demografische Diskriminierung
67. Hinzufügen von Merkmalen bei unschuldigen Menschen
68. Keine Akzeptanz bei Gemeinwohl-Überwachungs-Systemen
69. Barrieren jeden Tag Lebensentscheidungen zu treffen.
70. Große Risiken durch Fehler bei der „Datenüberwachung“
71. Streit über die Vereinbarkeit von (vorgeschrieben) Personendaten-Richtlinien
72. Möglicher Machtmissbrauch beim Zugriff auf Daten beim analysieren des Datenverkehr
73. Diskriminierung von speziellen ethnischen Gruppen.
74. Widerstand erzeugt aus Überwachungsangst bei DNA Datenbanken
75. Genetische Konstruktion von Tatverdächtigen
76. „Verlorengehen“ von Personenbezogenen Daten von einen System zum anderen.
77. Verlust der polizeilichen Legitimation

Stop Orwell 2020

gegen permanente Überwachung! Unschuldsvermutung bewahren!