

Finale Version des Manuskripts, die dem Verleger geschickt wurde. Persönliche Kopie der Autorin.
Bitte zitieren als: Zweig, K. A.: „Von der theoretischen Informatik zur Sozioinformatik --- und zurück“,
erschienen im Informatik Spektrum, 2015, 1, 28-30

Von der theoretischen Informatik zur Sozioinformatik – und zurück

Als digitaler Kopf wurde ich für meine interdisziplinäre Forschung mit dem besonderen Blick auf die möglichen Folgen der Digitalisierung für unsere Gesellschaft ausgezeichnet – diese Begründung mag auf den ersten Blick überraschen, denn ich leite an der TU Kaiserslautern als Professorin eine Arbeitsgruppe für Theoretische Informatik mit dem Thema „Graphentheorie und Analyse komplexer Netzwerke“. Wir Theoretiker stehen gemeinhin nicht unter Verdacht besonders anwendungsnah zu sein oder gar gesellschaftlich unmittelbar relevante Forschung zu betreiben. Tatsächlich genoss ich es nach meinem Erststudium der Biochemie mit vielen empirischen und zwangsläufig fehlerbehafteten Datenanalysen ganz besonders, mich in meinem zweiten Studium, der Informatik, hauptsächlich mit abstrakten Konzepten beschäftigen zu können. Schnell zeigte sich aber, dass die abstrakten Erkenntnisse der Graphentheorie es erlauben, sich sowohl mit hoch-theoretischen Fragestellungen zu beschäftigen als auch empirische Daten auf auffällige Muster hin zu untersuchen – und zwar auf Daten aller Fachdisziplinen im Rahmen der sich damals gerade neu etablierenden, sogenannten „Netzwerkwissenschaft“, die Methoden aus der statistischen Physik, der Soziologie, der Mathematik – natürlich insbesondere der Graphentheorie – und nicht zuletzt der Statistik zusammenfasst. Mit diesem Werkzeugset habe ich beispielsweise in den letzten Jahren krebshemmende Moleküle identifiziert [Uhlmann2012], gezeigt, dass selbst kleinste Mikroorganismen in den Weltmeeren ihre eigene Ökonomie besetzen und bewiesen, dass große soziale Netzwerkplattformen wie Facebook in der Lage sind, Beziehungen zwischen Paaren von Nichtmitgliedern abzuleiten [Horvat2012].

Das letzte Beispiel zeigt schon, dass die Netzwerkanalyse als Teil des Data Minings in Big Data, also der gezielten Suche nach auffälligen Mustern in großen Datenmengen, durchaus in der Lage ist, gesellschaftlich brisante Ergebnisse zu erzielen. Kollegen und Kolleginnen aus dem Feld der Netzwerkanalyse haben zusätzlich gezeigt, wie vorhersehbar wir in unserem Kommunikationsverhalten sind [Hidalgo2008], dass Mitglieder von sozialen Netzwerkplattformen unfreiwillig als homosexuell geoutet werden können [Jernigan2009] und auch andere Eigenschaften (Gehaltsklasse, Ausbildung, Parteizugehörigkeit) leicht ableitbar sind, selbst wenn diese von den Mitgliedern explizit geheim gehalten werden. Diese Resultate basieren darauf, dass wir Menschen uns im Wesentlichen unsere Freunde nach dem „Homophilie“-Prinzip aussuchen, also mit großer Wahrscheinlichkeit mit Personen befreundet sind, die ähnliche Eigenschaften haben wie wir. Ebenfalls große Auswirkungen könnte die Netzwerkanalyse noch in einem anderen Bereich haben: Amerikanische Kollegen wie Albert-László Barabási betonen stets, wie nützlich die Netzwerkanalyse sein kann, um Terroristen zu identifizieren [NetworkScience], und selbst SpiegelOnline bedient sich Methoden der Netzwerkanalyse, um ein deutsches „Terroristennetzwerk“ darzustellen (<http://www.spiegel.de/politik/deutschland/islamisten-daten-analyse-zum-netzwerk-in-deutschland-a-995153.html>).

Besonders erfolgreich werden Data Mining-Methoden dann, wenn sie nicht nur Daten aus einer Quelle nutzen, sondern mit Hilfe von APIs Daten aus unterschiedlichen Quellen zusammenführen. So konnte z.B. der für sich allein genommen völlig harmlose, pseudonymisierte Datensatz von Nutzer-Film-Bewertungsdaten der Firma Netflix zusammen mit öffentlich zugänglichen Daten von der Internet Movie Database (IMDB) genutzt werden, um Personen zu deanonymisieren, wenn sie denn dort ihren echten Namen benutzt hatten [Naranyan2008]. Während die Bewertungen auf der IMDB-Plattform freiwillig waren, enthielten die Netflixdaten einen Ausschnitt aller Bewertungsdaten – wobei nur Bewertungen für eine Teilmenge von Filmen dabei waren, die weder pornographischen

noch stark politischen Inhalts waren. Nichtsdestotrotz konnten nun aber mit diesen Daten also auch weitere Filmvorlieben aufgedeckt werden, als die, welche die Nutzer in der IMDB freiwillig und öffentlich bewertet hatten. Dies führte zu einer Klage gegen Netflix, in der eine als „Jane Doe“ bezeichnete, anonyme Klägerin ihre Befürchtung äußerte, damit unfreiwillig als Lesbe geoutet werden zu können. Die Klage wurde in einem Vergleich beigelegt und Netflix änderte seine Datenschutzrichtlinien. Als Nebeneffekt wurde die Forschung im Bereich Pseudonymisierungsstrategien stark angeregt und erfreut sich wachsender Popularität. Und hat Netflix aus diesem Vorfall wirklich etwas gelernt? Nun, eine eigentlich geplante zweite Veröffentlichung von Daten im Rahmen eines Wettbewerbs wurde abgesagt; 2013 aber veröffentlichte Netflix ein Video [<https://www.youtube.com/watch?v=VOBpprQdZTI>], in dem es ein neues Feature ankündigte: Nutzer können Filme, die ihnen gefallen haben, direkt auf ihrem Facebook-Zugang mit ihren Freunden teilen. Welche Vorhersagen und welche Data Mining-Strategien wird diese Datensammlung ermöglichen, wie sehr werden jetzt Freunde von Netflix-Nutzern mit passgenauer Filmwerbung bombardiert werden? Die oben genannten Beispiele und der Fakt, dass wir unsere Freunde unter Homophilie-Aspekten auswählen, lassen es erahnen.

Was passiert im Allgemeinen, wenn eine Data-Mining-Methoden eine hohe Falsch-Positiv-Rate aufweist, die viele unschuldige Personen zu Verdächtigen macht oder wenn die „harmlose“ Bewertung eines Films und das Versenden dieser Bewertung an ein Freundesnetzwerk die mutmaßlichen Vorlieben der Freunde demaskiert? Was passiert, wenn diese Methoden in Softwarepaketen zusätzlich jedem Laien zugänglich gemacht werden, und beliebige Anwender aus den verschiedenen Deanonymisierungsalgorithmen die falschen Schlüsse ziehen? Wer kann heutzutage wirklich noch beurteilen, was ein Algorithmus tut und welche Nebenwirkungen seine Resultate haben könnten? Wie wird die Digitalisierung unsere soziale Interaktion und Selbstorganisation verändern, wo müssen Gesetze regulierend eingreifen, wo wird die Gesellschaft selber Mittel und Wege finden, nicht gewünschtes Verhalten zu ächten und damit zu vermindern? Diese IT-basierten Technikfolgen gilt es abzuschätzen und im gesamtgesellschaftlichen Rahmen zu bewerten.

An der TU Kaiserslautern sind wir der Meinung, dass die direkte Technikfolgenabschätzung, also die Bedeutung und Verlässlichkeit der Resultate eines Algorithmus, nur ausgebildete Informatiker und Informatikerinnen überhaupt noch überblicken können. Um dann mögliche Reaktionen von Individuen, Gruppen, Organisationen oder der Gesellschaft als Ganzes vorherzusagen, reicht aber auch das rein informatische Wissen nicht aus: dafür ist es notwendig zu verstehen, wie Menschen sich in sozialen System selbst-organisieren, welchen Anreizen sie folgen und welchen Beschränkungen sie unterliegen. Dazu bedarf es beispielsweise Kenntnissen von spieltheoretischen Modellen aus den Wirtschaftswissenschaften, Modellen aus der statistischen Physik und Ansätze aus dem Bereich der Selbstorganisation komplexer Systeme, aber auch ein tiefes Verständnis der kognitiven Prozesse, die Menschen durchführen, um Entscheidungen zu fällen. Nicht zuletzt braucht es ein Verständnis für unser Rechtswesen und eine grundlegende Ausbildung in Ethik und Philosophie. Basierend auf diesem Ansatz habe ich federführend am Fachbereich den Studiengang „Sozioinformatik“ aufgebaut, der seit dem Wintersemester 2013 läuft und in dem sich inzwischen ca. 30 Studierende befinden – und kam so von der theoretischen Informatik zur Sozioinformatik.

Wie sieht nun ein typischer sozioinformatischer Ansatz zur möglichen Technikfolgenabschätzung aus? Das momentan erfolgreiche Bitcoinsystem kann da als Beispiel dienen: es ist eines von vielen Alternativen, die ein dezentrales Bezahlen anbieten, bei dem auf der einen Seite ein von allen Parteien getragenes Logsystem, die *Blockchain*, völlige Transparenz bietet, das aber gleichzeitig – bei professioneller Handhabung - auch Anonymität gewährt. Als Expertin in einem Diskussionspanel

wurde ich gefragt, ob ich das System für geeignet halte, um bundesweit eingesetzt zu werden. Eine solche Frage ist nicht leicht zu beantworten, aber die Kenntnis der menschlichen Psyche und das bisherige Verhalten von normalen Nutzern lässt erahnen, dass dem Normalsterblichen seine Anonymität in der Praxis weit weniger wichtig ist als in der Theorie. Es ist anzunehmen, dass Nutzer deren Lieblingspasswort bisher „123456“ oder „passwort“ [<http://www.pc-magazin.de/news/adobe-hack-passwoerter-top-100-zu-simpel-1893649.html>] war, auch ihre Bitcoin-Kontonummer (*Bitcoin Adresse*) nicht allzu oft wechseln werden, um ihre digitalen Spuren zu verwischen. Dazu kommt eine Erkenntnis aus den Wirtschaftswissenschaften: für beteiligte Firmen ist es wichtig, ihre Vertrauenswürdigkeit zu erhalten. Auch dies legt nahe, eine einmal gewählte Kontonummer beizubehalten, um Nutzer nicht zu verwirren. Dazu kommen dann noch langjährige Kundenbeziehungen, die auch in einer digitalen Welt hauptsächlich lokal sein werden, die Angabe von Adressdaten und vollständigen Namen auf Auktionsplattformen oder anderen Verkaufsseiten. Schon ist eine Deanonymisierung der meisten „normalen“ Nutzer von jedem, der die Bitcoin-Blockchain hat und ein früher oder später sicherlich ebenfalls verfügbares Deanonymisierungstool dafür installiert, zu machen – ähnlich wie im oben genannten Netflix-Fall. Der einzige, der anonym bleibt, ist der professionelle Nutzer, dem es ein großes Anliegen ist – darunter vermutlich insbesondere kriminelle Personen. Eine solche sozioinformatische Technikfolgenabschätzung vereinigt also ein profundes Wissen der algorithmischen Möglichkeiten der Deanonymisierung mit dem Wissen über kognitive Eigenschaften des normalen Nutzers und einem Wirtschaftsmodell, das im Internet auf Vertrauenswürdigkeit setzt. Das Beispiel zeigt insbesondere, dass die Art der Nutzung eines IT-Systems, das sich zu Beginn hauptsächlich unter professionellen Nutzern verbreitet, nicht einfach skaliert, wenn ein Großteil der gesamten Bevölkerung es nutzt.

Und hier tut sich nun auch wieder eine Chance auf für die theoretische Informatik: aufgrund der völlig neuen Möglichkeiten der digitalen Datengewinnung ergeben sich höchst spannende Fragen in der Graphentheorie und der Analyse komplexer Netzwerke. Zum Beispiel: Welche Schlüsse kann man aus reinen Bluetooth-Verbindungsdaten von Autos auf der Autobahn ziehen, selbst wenn weder der Halter noch die genauen GPS-Daten damit verknüpft sind? Wie sieht der Graph aus, der aus solchen Daten entsteht? Wie ist die Komplexität seiner Erkennung und unter welchen Umständen lassen sich welche Erkenntnisse daraus gewinnen? Und damit komme ich wieder von der Sozioinformatik in die theoretische Informatik zurück, wo man mit abstrakten Konzepten Grundlagenforschung betreiben kann, die später wieder Auswirkungen auf die Gesellschaft zeigen wird.

Diesen Kreislauf empfinde ich persönlich als enorm bereichernd, aber er zeigt auch, dass wir als Informatiker und Informatikerinnen – selbst wenn wir in der theoretischsten Ecke der Informatik arbeiten – für den kommenden Wandel eine enorme Verantwortung tragen. Die Forderung, dass wir unsere Methoden und Forschungsergebnisse besser kommunizieren müssen und auch die Technikfolgenabschätzung mit tragen müssen, ist beileibe nicht neu und die Gesellschaft für Informatik setzt sich, auch im Rahmen des Fachbereichs „Informatik und Gesellschaft“, immer wieder dafür ein. Doch bei der Geschwindigkeit, mit der neue Technologien und Algorithmen entwickelt werden, brauchen wir neue Wege der Kommunikation mit Politikern und Bürgern, und mehr Wissen darüber, wie Menschen sich in komplexen, sozialen Systemen organisieren, um unsere Gesellschaft auf ihrem Weg in die Digitalisierung kompetent zu begleiten.

Referenzen:

[Hidalgo2008] Hidalgo, C. A. & Rodriguez-Sickert, C. The dynamics of a mobile phone network *Physica A*, 2008, 387, 3017-3024

[Horvat2012] Horvát, E.-Á.; Hanselmann, M.; Hamprecht, F. A. & Zweig, K. A. One plus one makes three (for social networks) PLoS ONE, 2012, 7, e34740

[Jernigan2009] Jernigan, C. & Mistree, B. "Gaydar: Facebook friendships expose sexual orientation" First Monday [Online], 2009, 14,
<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2611/2302>

[Narayan2008] Narayanan, A. & Shmatikov, V. Robust De-anonymization of Large Sparse Datasets (How to break Anonymity of the Netflix Prize Data set) Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP'08), 2008, p. 111-125

[NetworkScience] Kapitel 1 des online-Lehrbuches „Network Science“, Version vom 18.11.2014,
http://barabasilab.neu.edu/networksciencebook/download/network_science_November_Ch1_2012.pdf

[Uhlmann2012] Uhlmann, S.; Mannsperger, H.; Zhang, J. D.; Horvat, E.-Á.; Schmidt, C.; Küblbeck, M.; Ward, A.; Tschulena, U.; Zweig, K.; Korf, U.; Wiemann, S. & Sahin, Ö. Global miRNA Regulation of A Local Protein Network: Case Study with the EGFR-Driven Cell Cycle Network in Breast Cancer Molecular Systems Biology, 2012, 8, 570