

Verein löst sich auf Umstrittene An'Nur-Moschee ist am Ende

WINTERTHUR Lichter löschen beim Kulturverein An'Nur, der die gleichnamige Moschee in Winterthur betreibt: Nach dem Fastenmonat Ramadan im Juni wird der Verein aufgelöst. Atef Sahnoun vom An'Nur-Verein bestätigte im «SonntagsBlick» den Schritt. Es habe keinen Sinn mehr, wird er zitiert. Die Moschee war in der Vergangenheit wiederholt in die Schlagzeilen geraten – zuletzt im Februar nach der Festnahme von zehn Personen wegen eines Angriffs auf zwei Glaubensbrüder, die interne Informationen an einen Journalisten weitergegeben haben sollen.

Die Schliessung der umstrittenen Moschee im Winterthurer Stadtteil Hegi war bereits per Ende 2016 in Aussicht gestellt worden, nachdem sich die Vermieterin geweigert hatte, den langjährigen Mietvertrag zu erneuern. Sahnoun machte damals die Medien verantwortlich: «Die reisserische Berichterstattung ist schuld daran, dass unser Mietvertrag nicht verlängert wurde.»

Ende November tauchten auf Litfasssäulen in Winterthur Plakate mit dem Titel «Moscheeretung» auf. Mit Spenden sollte die Moschee für Gläubige gerettet werden. Anfang 2017 schliesslich einigten sich der Kulturverein An'Nur und die Vermieterin vor der Schlichtungsbehörde auf eine letzte Erstreckung des Mietverhältnisses. Laut Sahnoun haben die Leute Angst, dem Verein Quartier zu bieten.

Razzia und Dschihad-Reisende

Die Moschee sorgte auch im Zusammenhang mit Dschihad-Reisenden für Schlagzeilen. Mehrere Jugendliche waren nach Syrien gereist und hatten sich der Terrormiliz Islamischer Staat (IS) angeschlossen. Alle sollen in der An'Nur-Moschee radikalisiert worden sein. Am 2. November 2016 führte die Polizei eine Razzia durch und verhaftete insgesamt vier Personen – darunter einen äthiopischen Imam. Dieser soll in einer Predigt zur Tötung von Muslimen aufgerufen haben. (sda)

Das Sorgenkind Wasserkraft

Die Wasserkraftwerke sind in Not, daran ändert auch das Ja zur Energiestrategie nichts. In den nächsten Monaten ringt die Politik um weitere Unterstützungsmassnahmen. Dabei stehen auch die Wasserzinsen zur Diskussion.

VON DOMINIC WIRTH

180 Millionen Franken pro Jahr: So viel zusätzliches Geld steht nach dem Ja zur Energiestrategie für die Betreiber von Wasserkraftwerken in Zukunft bereit. Allerdings steht jetzt schon fest, dass es dabei nicht bleiben wird in Sachen Unterstützungsmassnahmen für die Wasserkraft. Deren Anlagen waren schon bis anhin der wichtigste Pfeiler der inländischen Stromproduktion; knapp 60 Prozent des Schweizer Stroms stammen aus den 600 Wasserkraftwerken. Und nun, da die Schweiz den Atomausstieg beschlossen hat, wird die Wasserkraft noch wichtiger.

Entsprechend gross ist der politische Wille, den Stromkonzernen zusätzlich unter die Arme zu greifen. Vor allem den Wasserkraftwerkbesitzern, die ihren Strom nicht an gebundene Endkunden, sondern im freien Markt verkaufen müssen, machen die tiefen Preisen zu schaffen. In den nächsten Monaten wird es darum gehen, auf welche Art sie weiter unterstützt werden sollen. Dabei kommt neben zusätzlichen Subventionen mit den Wasserzinsen bald ein explosives Thema ins Spiel. Mit ihnen entschädigen die Stromkonzerne die Standortkantone für die Nutzung der Ressource Wasser. Ausserdem befassen sich die zuständigen Parlamentskommissionen auch bereits mit der Ausgestaltung der Rahmenbedingungen für den Strommarkt der Zukunft.

Umstrittenes Modell

Vorerst steht aber die Frage nach den kurzfristigen Zusatzmassnahmen im Zentrum. Bereits heute, wenn die Sommersession des eidgenössischen Parlaments beginnt, fällt hier ein erster Entscheid. Der Nationalrat beschliesst, wie es mit den Wasserkraft-Hilfsplänen seiner Energiekommission weitergehen soll. Die hatte Ende April überraschend beschlossen, Haushalte und KMU zusätzlich zur Kasse zu bit-



Nach dem Ja zur Energiestrategie wird die Wasserkraft in Zukunft noch stärker das Rückgrat der Schweizer Stromversorger sein. Über die Unterstützungsmassnahmen ist man sich in der Politik bis jetzt aber noch nicht einig.

Bild Key

ten, um die Wasserkraft zu stützen. Die Idee: Kleine Verbraucher sollen künftig nur noch Wasserkraftstrom erhalten – und das zu einem Preis, der die Gestehungskosten der Hersteller deckt und eine Marge beinhaltet.

Allerdings ist der Weg zu diesem Modell noch weit. Zum einen wurde es von der Kommissionsmehrheit auch unterstützt, um im parlamentarischen Prozess eine Differenz zum Ständerat zu schaffen, der einen anderen Weg einschlagen wollte. Zum anderen schwindet die Unterstützung. Heute dürfte sich die Mehrheit des Nationalrats darum für einen Antrag des Berner FDP-Nationalrats Christian Wasserfallen aussprechen. Dieser schlägt vor, die Diskussion über die zusätzliche Wasserkraftunterstützung noch einmal in die Kommission zurückzuschicken. Der Hinter-

grund: Das nun vorliegende Modell wurde bei der Beratung der Strategie Stromnetze ins Spiel gebracht. Wasserfallen findet, dass es dort nichts zu suchen hat, weil es bei diesem Geschäft nicht um die Grundversorgung geht. «Dennoch hat man – notabene ohne Vernehmlassung – ein Konzept ins Spiel gebracht, dessen Auswirkungen kaum abschätzbar sind. Das ist unseriös», sagt er. Und nachdem in der Kommission der Widerstand gegen das Modell noch vor allem aus den Reihen der FDP gekommen war, signalisieren mittlerweile Politiker verschiedener Parteien, dass sie auch dafür sind, das Ganze noch einmal ausführlich zu durchleuchten.

Gezerre um Wasserzinsen

In den nächsten Wochen wird Bundesrätin Doris Leuthard ein weiteres,

hochbrisantes Thema in die Wasserkraftdiskussion einbringen: die Zukunft der Wasserzinsen. Diese spülen den Standortkantonen und -gemeinden jährlich über 500 Millionen Franken in die Kasse. Gerade in Graubünden und im Wallis sind diese Einnahmen zentral; in vielen Bündner Gemeinden machen sie 20 bis 40 Prozent der Gesamteinnahmen aus. In den fetten Jahren, als die Wasserkraftwerke den Betreibern hohe Gewinne einbrachten, gab diese Abgabe kaum zu reden. Das hat sich unterdessen geändert. Die Diskussionen darüber, wie es mit den Wasserzinsen weitergehen soll, laufen schon länger. Bilaterale Gespräche zwischen den Wasserkantonen und der Strombranche blieben allerdings ohne Ergebnis, weil die Fronten derart verhärtet sind.

Das Internet muss nicht das Ende der ärztlichen Schweigepflicht sein

Letzte Woche hat das Bundesgericht die Verurteilung eines Mediziners bestätigt, der einen vertrauensärztlichen Bericht an den Arbeitgeber eines Patienten weitergeleitet hatte. Damit verletzte er das strafrechtlich geschützte ärztliche Berufsgeheimnis: Ohne Einwilligung dürfen Ärztinnen und Ärzte Patientendaten Dritten nicht preisgeben. Patientinnen und Patienten sollen sich darauf verlassen können, dass ihre Gesundheitsinformationen vertraulich bleiben.

Doch in der digitalisierten Welt wird dieser Geheimnisschutz zur reinen Fiktion. Nicht zuletzt, um ihre immer umfangreicheren administrativen Aufgaben zu delegieren, lagern Ärzte und Spitäler ihre Patientendaten an IT-Unternehmen im In- und Ausland aus oder nutzen Clouddienste für deren Verwaltung und Archivierung. Damit nehmen sie in Kauf, dass Dritte Einblick in geheimnissgeschützte Informationen nehmen könnten.

Um einer strafrechtlichen Verurteilung zu entgehen, wird der Begriff der «Hilfspersonen», mit denen der Arzt das Berufsgeheimnis teilen darf, vom Pflegefachpersonal einfach auf IT-Unternehmen und Cloudanbieter ausgedehnt. Doch diese Praxis, das hat ein viel beachtetes Gutachten von Wolfgang Wohlers, Professor für Strafrecht an der Universität Basel, nun aufgezeigt, lässt sich nicht rechtfertigen. Ärzte und Spitäler sind als Geheimnis-

Das Arztgeheimnis, das eigentlich ein Patientengeheimnis ist, gerät im digitalen Zeitalter in Bedrängnis. Das sollten wir nicht kampflos hinnehmen.

VON BRUNO BAERISWYL*

träger dazu verpflichtet, das ihnen in ihrer Berufsausübung anvertraute Geheimnis zu wahren. Geheimnisschutzherr ist allein der Patient oder die Patientin. Nur wenn sie ihre Einwilligung erteilen, oder wenn sich ausschliessen lässt, dass der Informatikdienstleister Zugriff auf die ausgelagerten Daten haben könnte, ist Outsourcing in der aktuellen Rechtslage überhaupt möglich.

Mit der Einführung des elektronischen Patientendossiers, dem automatisierten Austausch von Patientendaten und der Integration unterschiedlicher Systeme schreitet die Digitalisierung im Gesundheitswesen rasant voran. Aus wirtschaftlichen Gründen kann und soll auf das Outsourcing nicht verzichtet werden: Bedeutet dies das unaufhaltbare Ende des Patientengeheim-

nisses? Ja, wenn man die aktuelle Situation einfach hinnimmt. Nein, wenn man Massnahmen in Erwägung zieht, die die Möglichkeit einschränken, dass der Informatikdienstleister von den Daten Kenntnis nehmen könnte: In erster Linie durch eine Verschlüsselung der Daten, wobei das Schlüsselmanagement beim Spital oder beim Arzt liegen muss. Im Einzelfall könnte die Nutzung des Schlüssels auch vertraglich eingeschränkt werden.

Soll das Patientengeheimnis nicht der Digitalisierung geopfert werden, müssen wir jetzt handeln. Die jüngsten Cyberattacken auf IT-Systeme verschiedener Gesundheitsdienste haben gezeigt, wie verletzlich Gesundheitsdaten gegenüber Hackerangriffen sind. Neben der pragmatischen Umsetzung der notwendigen Sicherheitsmassnahmen sollten wir aber auch darüber nachdenken, wie ein zeitgemässer Geheimnisschutz im Gesundheitswesen heute zu gestalten wäre. Das strafrechtliche Konstrukt der individuellen Einwilligung erscheint im digitalen Umfeld viel zu umständlich. An seine Stelle könnte ein Geheimnisschutz treten, der den Institutionen im Gesundheitswesen und ihren Informatikdienstleistern genaue datenschutzrechtliche Rahmenbedingungen vorgibt – an den Datenschutzbehörden wäre es dann, diese von Amtes wegen zu überprüfen.

* Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich

Bundesrat Parmelin muss Cyber-Abwehr nachrüsten

Das Verteidigungsdepartement sei für Cyber-Angriffe nur ungenügend gerüstet, halten Prüfer des Bundes fest. Bundesrat Parmelin will nun 100 Millionen Franken jährlich in die Abwehr stecken.

VON FABIAN FELLMANN

BERN Das Schadprogramm WannaCry hat in Erinnerung gerufen, wie verletzlich kritische Infrastrukturen, etwa Spitäler, für elektronische Angriffe sind. Trotzdem ist das Eidgenössische Verteidigungsdepartement für grössere Attacken nur ungenügend gerüstet. Zu diesem Schluss kommt die departementsinterne Revisionsstelle. Die Durchhaltefähigkeit sei bei längeren oder grösseren Cyber-Angriffen auf die Schweiz «gering». Die Stellvertretung von Schlüsselpersonen etwa sei nicht sichergestellt. Dies heisst es in einem Bericht, den SVP-Bundesrat Guy Parmelin nach der Übernahme des Verteidigungsdepartements bestellt hatte. Das Papier hat das Departement vor wenigen Tagen auf seiner Website veröffentlicht; es datiert vom September 2016.

Nun plant der Verteidigungsminister, die Ressourcen für die Bekämpfung von Cyber-Angriffen zu erhöhen. In Zukunft dürften zwei Prozent des Departementsbudgets in die Cyber-Abwehr fliessen; das entspricht rund 100 Millionen Franken jährlich. Das erwähnte Parmelin Anfang Mai an einer Konfe-

renz des Sicherheitsverbands Schweiz, wie sein Departement jetzt bestätigt. Laut Aussagen Parmelins vom März soll die Zahl der Stellen bis 2020 von derzeit rund 50 auf 150 wachsen.

«Weitere Anpassungen nötig»

Erste Schritte zur Stärkung der Durchhaltefähigkeit hat der Bundesrat bereits beschlossen: 30 befristete Stellen in der Verwaltung wurden in unbefristete umgewandelt. Dies deckt jedoch nur die nötigste tägliche Arbeit ab, wie die Inspektoren festhalten. Weitere Aufstockungen des Budgets behält sich das Departement denn auch vor: «Im Anschluss an die Revision der Nationalen Cyber-Strategie werden weitere Anpassungen nötig sein», sagt Sprecherin Karin Suini. Mit der Nationalen Cyber-Strategie will der Bund kritische elektronische Infrastruktur schützen.

Das Verteidigungsdepartement arbeitet derzeit an der Umsetzung seines eigenen «Aktionsplans Cyber Defense», den Parmelin im April 2016 nach einem Hacker-Angriff auf den Bundesrüstungsbetrieb Ruag bestellt hat. Unter anderem lässt er ein neues Koordinationsorgan im Departement definitiv einrichten. Ziel des Aktionsplans ist es laut Suini, «permanent und in allen Lagen» die Systeme der Verteidigung zu schützen, militärische und nachrichtendienstliche Operationen im Cyber-Raum zu unterstützen und den zivilen Behörden bei Angriffen auf kritische Infrastrukturen Hilfe leisten zu können.