

**ONLINE
PRESSE-
GESPRÄCH**
13.03.2023

DARK PATTERNS: MANIPULATION IM NETZ!

AK Studie analysiert Dark Patterns im Alltag – Gängige Praxis: Durch Gestaltungstricks sollen Konsument:innen zu bestimmten Verhalten animiert werden – Im Anmarsch: Emotionserkennung, verletzt Konsument:innenschutz und Menschenwürde – AK will mehr digitale Fairness

DANIELA ZIMMER

Konsument:innenschutzexpertin, AK Wien

LOUISE BELTZUNG

Studienautorin, Österreichisches Institut für angewandte
Telekommunikation (ÖIAT)

1100001
öiat



Dark Patterns im Netz: Achtung, verlorene Zeit, verlorenes Geld, verlorene Daten!

Manipulative Praktiken im Netz werden immer raffinierter – Dark Patterns beeinträchtigen die digitale Selbstbestimmung der Konsument:innen massiv – Akute Manipulationsgefahr durch Emotionserkennung – AK will digitale Fairness in der EU

Es ist ein Klacks, ein Konto zu registrieren. Es wird aber erschwert, die eigenen Daten zu löschen. Der Button „Allen Cookies zustimmen“ ist feuerrot, der Button „Nur erforderliche Cookies“ ist fast unsichtbar. Klicks im Netz können es in sich haben – und das ist alles kein Zufall. Der Trick hinter all diesen Klicks heißt Dark Patterns – dunkle Muster. Mit diesen Gestaltungsmustern/Webdesigns sollen User:innen im Web zu einem bestimmten Verhalten animiert werden – so wie es die Anbieter wollen. Apps und Webseiten strotzen nur so vor Praktiken, die die digitale Selbstbestimmung der Konsument:innen massiv beeinträchtigen und sie zu ungewollten Entscheidungen verleiten oder drängen: verschachtelte Menüs, Psycho-Tricks, Countdowns & Co. Das zeigt eine von der AK beim Österreichischen Institut für Telekommunikation (ÖIAT) beauftragte Studie.

AK Konsument:innenschutzexpertin Daniela Zimmer: „Konsument:innen werden täglich durch technische Tricks im Web manipuliert. Dabei werden ihnen Daten und Geld abgeluchst. Der Kunde/die Kundin ist im Web nicht König:in, sondern immer öfter vor allem Datenquelle und Manipulationsobjekt. Ganz schlimm und auch schon verbreitet, die Emotionen von Konsument:innen zu erkennen und gezielt zu stimulieren. Anbieter schleichen sich da in die intimste Privatsphäre ein.“

ÖIAT-Studienautorin Louise Beltzung: „Internationale Studien bestätigen, was auch wir sehen: Dark Patterns sind weit verbreitet. Auf unterschiedlichste Art wird versucht, dass Konsument:innen Entscheidungen möglichst impulsiv und rasch treffen, auch wenn das möglicherweise nicht in ihrem besten Interesse liegt. Gerade für vulnerable Konsument:innen ist das ein Problem.“

Die EU-Kommission hat aktuell eine Initiative zur „Digitalen Fairness“ gestartet und will unfaire Online-Praktiken bekämpfen. Das ist höchst an der Zeit, aber die AK befürchtet: Der Weg zu mehr digitaler Selbstbestimmung für Konsument:innen ist weit, weil die EU-Regulierung besorgniserregenden Markttrends weit hinterherhinkt, etwa der Emotionserkennung fürs personalisierte „Gefühlsmarketing“. Die AK fordert ein Verbot von Geschäftspraktiken, die die Menschenwürde berühren.

Dark Patterns im Alltag von Konsument:innen

Das Österreichische Institut für Telekommunikation (ÖIAT) hat sich im Auftrag der AK auf die Suche nach den „dunklen Mustern“ – Dark Patterns – von Online-Anbietern gemacht: Erhoben wurden illustrative Web-Beispiele und internationale Studien, die sich diesem Phänomen widmen.

Dark Patterns haben System

Schon 2010 kritisierte der Internetexperte für „User Experience“/„Nutzerfreundlichkeit“ Harry Brignull, dass Websites und Apps Design einsetzen, um User:innen zu manipulieren. Er führte den Begriff „Dark Patterns“ ein und bezeichnete damit die Taktik, die Schnittstelle zu den User:innen so zu gestalten, dass diese ihr Verhalten entgegen ihren ursprünglichen Absichten oder Interessen ändern – über Manipulation, Irreführung oder Zwang. Inzwischen bedienen sich Online-Anbieter unzähliger unfairer psychologischer Tricks bei ihren Apps, Gerätemenüs, Plattformen oder Websites. Design und Prozesse

werden so gestaltet, dass Konsument:innen zu Entscheidungen unbewusst gedrängt werden. Es ist schwieriger, ein Abo zu kündigen, als eines abzuschließen. Ein Konto oder eine Registrierung ist ruckzuck erledigt. Die eigenen Daten löschen gleicht hingegen einer Online-Odyssee. Der Button „Allen Cookies zustimmen“ ist signalrot, der daneben mit „Nur erforderliche Cookies“ ist blassgrau. Kein Zufall, sondern alles System. Denn IT und Marketing arbeiten beim Webdesign eng zusammen.

Sicher, auch klassische Vermarktung versucht Konsument:innen zu beeinflussen und sie zu Spontankäufen zu animieren. Aber im Internet sind Dark Patterns gefährlichere Kaliber: Anbieter haben – dank massenhafter Personendaten, Algorithmen, Künstliche Intelligenz (KI) und ausgeklügeltem Webseitendesign – besonders machtvolle Mittel, das User:innenverhalten auch unbemerkt zu steuern. Durch Klassifizierung nach hunderten persönlichen Merkmalen in Kombination mit neuropsychologischen Erkenntnissen und technischen Gestaltungsmöglichkeiten sehen sich Konsument:innen immer dreisteren Manipulationsversuchen und Abhängigkeiten ausgesetzt.

Manipulation im Netz – was Dark Patterns bewirken

Dark Patterns bewirken, dass User:innen mehr Daten mit einem Unternehmen teilen, mehr Geld ausgeben oder auch Entscheidungen treffen, die nicht in ihrem Interesse sind. In den späten 1970er Jahren wurden die Grenzen der Rationalität von Menschen untersucht: Sind Menschen unsicher bzw. fehlen ihnen Infos oder kognitive Fähigkeiten, verhalten sie sich irrational – ihren Interessen zuwiderlaufend. Verhaltensökonom:innen kritisieren Lenkungsversuche (Nudges) schon lange. Das kann Personen dabei helfen „für sie bessere Entscheidungen zu treffen“ oder das blanke Gegenteil bewirken. Der menschliche Hang zu automatischen, impulsiven, intuitiven Entscheidungen wird dabei ausgenutzt.

Aus der (Psycho)Trickkiste: Anbieter wollen, Konsument:innen tun!

Warenkorbtrick: Produkte oder Extraservices, die nicht ausgewählt wurden, werden wie ein Kuckucksei einfach in den Warenkorb gelegt.

Überladene Websites: User:innen werden mit Unmengen an Infos und Optionen konfrontiert, um beispielsweise mehr Daten preiszugeben, als sie wollen. Designelemente (unklare Gliederung, Unterebenen) lenken gezielt ab und verwirren. Überlange Texte desinformieren. Overchoice, also die Auswahl aus zu vielen verwirrenden Optionen, überfordert Konsument:innen. Statt eine Wahl zu treffen, werden sie in die Inaktivität getrieben.

Versteckte Infos: Informationen werden für Konsument:innen „direkt vor der Nase“ versteckt. So werden etwa über Farbauswahlen (leuchtend oder blass) User:innen dazu bewegt, spontan nur die eine Option zu wählen, die der Anbieter will.

Privatsphäre-Irrgarten: User:innen müssen durch ein Labyrinth, um zu gut versteckten Privacy-Einstellungen zu finden. Der Trick heißt nach dem Facebook-Gründer Zuckerberg „Privacy Zuckering“.

Versteckte Werbungen: Sie verleiten dazu, auf etwas zu klicken, was nicht als Werbung gekennzeichnet ist.

Störende Unterbrechungen: Konsument:innen werden durch das Aufpoppen von Pop Ups unterbrochen. Diese drängen zu Handlungen, etwa dem Download einer App.

Verschleierte Preise: Durch den Einsatz von „Zwischenwährungen“ (virtuellen Währungen in Videospiele oder auf Datingplattformen), die Einblendung von Kosten und Extragebühren erst ganz am Ende des Bestellvorgangs.

Verhinderung von Preis- und Produktvergleichen: Auch über Design kann verhindert werden, dass User:innen auf einfache Art vergleichen können, etwa, weil Angebote unvollständig beschrieben sind oder die gewählten Mengenangaben zur Preisindikation speziell und unüblich gewählt werden.

Hervorhebungen: Spielwiese für Designer in Bezug auf Farben, Schriftgröße, Größe von Schaltflächen, Positionierungen, um etwa bei einzuholenden Zustimmungen gegen die Interessen der User:innen zu arbeiten; User:innen sollen auch falschen grafischen Codes auf den Leim gehen (zum Beispiel ein Vertrauenswürdigkeit suggerierendes Vorhängeschloß für ein nicht sicheres Interface).

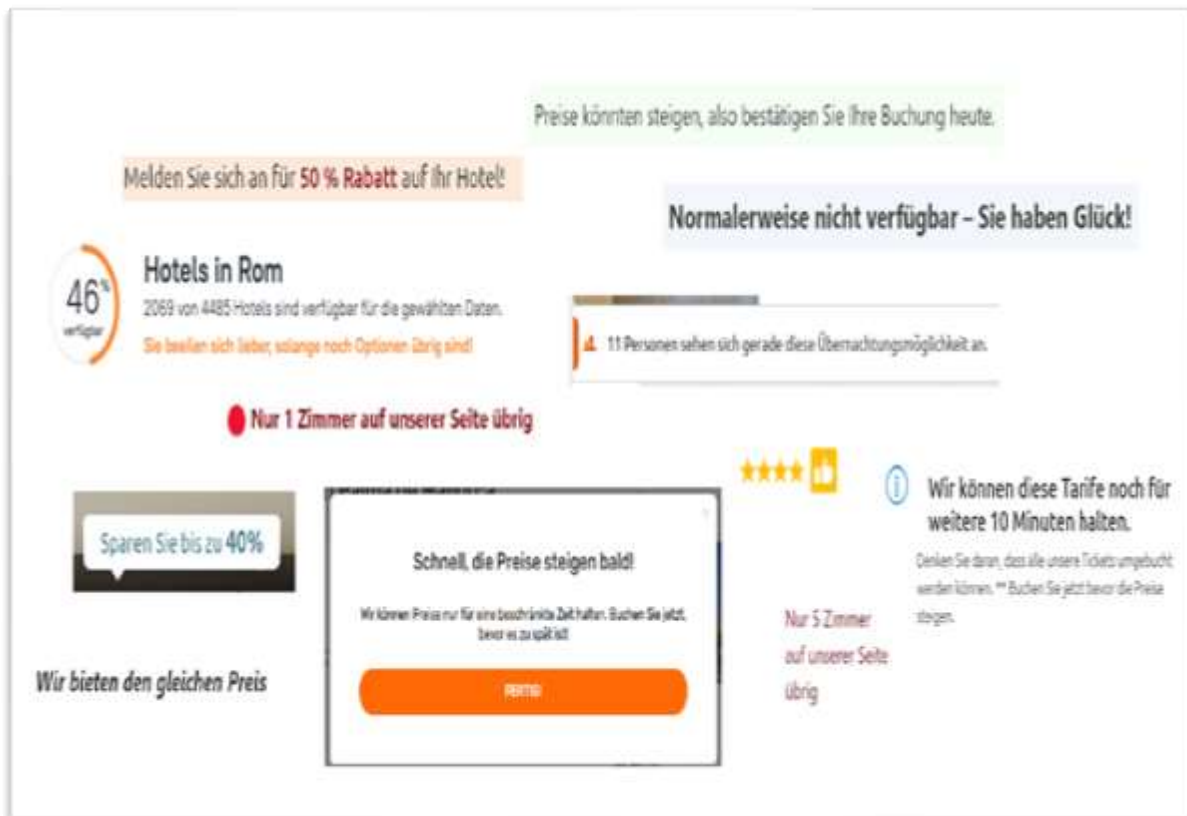
Zeitdruck, simulierte Knappheit und Countdowns: Aktivitätsmeldungen („7 andere schauen sich das Produkt an“) und Knappheitshinweise („geringer Vorrat“, „nur mehr 2 auf Lager“) spielen mit der Angst der User:innen, etwas zu verpassen. Zustimmungserklärungen werden platziert, wo User:innen bereits ungeduldig den Prozess abschließen wollen. Countdown-Timer, zeitlich begrenzte Aktionen, Blinken, Pop-Ups erzeugen übermäßigen Druck.

Ab- und Registrierzwang: Versteckte oder vorausgewählte Abos (Dienstleistungen, Newsletter) und erzwungene Verlängerung derselben. Persönliche Registrierung wird User:innen ohne triftigen oder mit einem bloß vorgeschützten Grund abverlangt.

Beispiel: Schnell zuschlagen – Countdowns, Rabatte & Co.

So werden Konsument:innen häufig manipuliert, damit sie schnell buchen oder etwas kaufen: versteckte Informationen, falsche Hierarchien, nachteilige Vorauswahlen, Bedrängen (etwa durch Countdown-Timer oder zeitlich begrenzte Angebote), erschwerte Stornierungen, erzwungene Registrierungen.

Manipulationen auf Hotelplattformen – gesammelte Beispiele



Wenn Emotion auf Business trifft

Die Werbeindustrie arbeitet schon immer daran, Angebote und Werbungen perfekt auf Konsument:innen abzustimmen. Doch wie weit darf sie dabei gehen? „Wirtschaft des Einfühlungsvermögens“, „Persönlichere User Experiences“, „menschlicheres, empathisches Marketing“ nennen es KI-Anbieter, die Emotionen von Konsument:innen erkennen und gezielt stimulieren wollen, sich aber damit in die intimste Privatsphäre einschleichen. Handys, Sprachassistenten oder Wearables liefern dafür jedenfalls genug Bild-, Audio- und andere biometrische Daten, um Mimik, Sprache, Gestik nach Ausdrücken wie Freude, Wut, Ekel, Furcht, Überraschung usw. zu untersuchen. Zahlreiche Tech-Giganten investieren massiv in Emotionserkennungs-Software. Apples Kauf von Emotient, ein darauf spezialisiertes Start-Up, ist einer der vielen Hinweise, dass die Werbeindustrie nun auch unsere Gefühle vermessen will.

„Mitfühlende“ („empathische“) KI entwickelt hoch personalisierte Werbebotschaften. Chatbots prüfen die Persönlichkeitsmerkmale von Konsument:innen und wie sie auf Mitarbeiter:innen, den Firmenauftritt und Produkte emotional reagieren. Stirnrunzeln, frustrierte Gesichtsausdrücke – und schon werden Produkte, Preise oder Präsentation überdacht und geändert. Amazon hat neue Funktionen patentiert, mit deren Hilfe Echo-Geräte erkennen, ob jemand krank ist – wie etwa Stimmprofile, die auf eine verstopfte Nase hinweisen. Empathische KI reagiert umgehend mit einem Hühnersuppenrezept oder dem Lieferangebot von Hustenbonbons. Für die Werbeindustrie ist das verheißungsvoll, für die Betroffenen droht akute Manipulationsgefahr und letztlich auch die Missachtung ihrer Menschenwürde.



[Screenshot/Emotient Analytics - How Apple Could Use Emotient \(businessinsider.com\)](#)

Viele beliebte Apps & Online-Shops mit mindestens einem Design-Trick

Die EU sagt Dark Patterns den Kampf an. Der EU-Kommission ist dieses Missbrauchspotenzial bewusst. Eine von der EU beauftragte Studie „dark patterns and manipulative personalisation“ zeigt: 97 Prozent der beliebtesten Apps und Online-Shops setzen zumindest einen Design-Trick ein. Unseriöse Techniken kommen bei Apps und Websites gleichermaßen vor. Der Studie zufolge reicht der aktuelle Rechtsrahmen (und sein Vollzug) nicht aus, um Konsument:innen vor einer ihnen nicht bewussten Beeinflussung ihrer Entscheidungen zu schützen. Laut EU-Kommission fehlt es Konsument:innen ganz oft am Bewusstsein für Manipulationsabsichten und auch an der Fähigkeit, diese Praktiken im Alltag zu erkennen. Noch bedenklicher: Konsument:innen scheinen unlautere Praktiken als normale Interneterfahrung zu akzeptieren.

Die Folgen von Dark Patterns sind vor allem verlorene Zeit und verlorenes Geld. Längerfristig erwartet die AK, dass die Privatsphäre der Konsument:innen und letztlich auch die Menschenwürde noch mehr leidet. Die Digitalökonomie gewinnt durch den Einsatz von Daten, Algorithmen und KI immer mehr Macht über Konsument:innen. KI-Dienstleister versprechen über Emotionserkennung und Analysen der bisherigen Verhaltens- und Transaktionsdaten punktgenau jene Momente im Leben von Frau/Herrn X zu bestimmen, in denen sie am empfänglichsten für ein bestimmtes Produkt sind. Es sind nicht nur Belohnungs- und Glückssituationen, sondern vor allem jene, in denen Konsument:innen sehr verletzlich sind: Angebote als willkommene Ablenkung, Rettungsanker oder Trost.

Aktuelle Gesetze und Vorschriften mit „Schwachstellen“

UWG – Gesetz gegen den Unlauteren Wettbewerb: Der Begriff Dark Patterns mag relativ neu sein, das Verbot von aggressiven und irreführenden Werbe- und Vertriebspraktiken nach dem UWG bzw. der Unerlaubte Geschäftspraktiken-Richtlinie der EU gibt es schon lange. Probleme, diese Vorschriften

rechtssicher auf Online-Betreiber anzuwenden und Vollzugsdefizite führen dazu, dass Internetnutzer:innen unfairen Tricks trotzdem auf Schritt und Tritt begegnen.

Datenschutzgrundverordnung: Ähnlich verhält es sich mit irreführenden Cookie Bannern. Nach der Datenschutzgrundverordnung können Online-Nutzer:innen nur vollständig informiert und freiwillig kommerziellen Datennutzungen wirksam zustimmen. Dennoch musste der Datenschutzverein NOYB bei Datenschutzbehörden hunderte Beschwerden einbringen, weil ebenso viele Websites die irreführenden Banner der Firma „One Trust“ nutzen.

Neue Digital-Vorschriften: Das Digitale Dienste Gesetz der EU setzt immerhin Online-Plattformen Grenzen. Sie dürfen ihre Online-Schnittstellen nicht so gestalten, dass Nutzer:innen „getäuscht, manipuliert oder anderweitig in ihrer Fähigkeit, freie und informierte Entscheidungen zu treffen, behindert werden“. Der EU-Rechtsakt erwähnt etwa schwer änderbare Standardeinstellungen oder Täuschungen, um Nutzer:innen zu Transaktionen zu drängen. Er verbietet beispielsweise Praktiken, wie Auswahlmöglichkeiten stärker hervorheben, wenn Nutzer:innen zur Auswahl aufgefordert werden oder wiederholte Aufforderung, eine Auswahl zu treffen, wenn diese bereits getroffen wurde. Oder kein zeitlicher (Countdowns, Zahl anderer Interessent:innen, geringe Zahl verfügbarer Stücke) und inhaltlicher Druck.

Was die AK will: Digitale Fairness – selbstbestimmte Konsument:innen respektieren, sensible Daten schützen und Emotionserkennung verbieten!

Die AK begrüßt zwar, dass sich die EU mit ihrem Digitalen Dienste Gesetz und ihrer „Digitalen Fairness“-Initiative nun den unzähligen Dark Patterns widmet. Diese stellen aber bei weitem nicht alle unfairen Praktiken im Web dar. IT und Marketing bilden immer öfter eine Allianz mit den Neurowissenschaften und der Psychologie. Was wir wie, wann und warum auf Bildschirmflächen sehen, soll schon bald hochindividualisiert auf unsere jeweiligen Emotionen abgestimmt sein. Emotionserkennung für kommerzielle Zwecke verletzt nicht nur elementare Prinzipien des Konsument:innenschutzes, sondern vielmehr die Menschenwürde. Derartige Praktiken dürfen sich gar nicht ausbreiten, sondern müssen verboten werden, fordert die AK.

Für die AK ist die „Digitale Fairness“ Initiative der EU hoch an der Zeit. Rechtsanpassungen im bestehenden Rechtsrahmen wie Verbraucherrechte-Richtlinie, Unlautere Geschäftspraktiken-Richtlinie und missbräuchliche Klauseln-Richtlinie sind positiv. Es sind aber strengere gesetzliche Maßnahmen nötig, um digitale Fairness als Konsument:innenschutzstandard durchzusetzen.

Zimmer: „Es braucht mehrere Hebel. So ist etwa eine breite Debatte zur Frage, was darf Digitalmarketing und was ist unverantwortliche Manipulation? Detaillierte Konsument:innenprofile können für die Konzeption von Dark Patterns und gegen die User:innen eingesetzt werden. Die psychologischen Effekte von Tricks kann jederzeit an ahnungslosen User:innen getestet werden. Die Verbotliste unlauterer digitaler Praktiken für Online-Plattformen im Digitalen Dienste Gesetz der EU ist ein guter Beginn, aber ausbaufähig.“

Konkret verlangt die AK:

Digitale Fairness gegenüber Konsument:innen und Respekt vor ihrer Privatsphäre: Fatal ist, wenn Dark Patterns mit Personalisierungspraktiken kombiniert werden, um die Schwächen und Lebenssituation einer Person auszunutzen. Regulierung von Dark Patterns bedeutet daher, auch den zulässigen Umfang der Datensammlung für und den Einsatz von personalisierten Angeboten und Werbung zu begrenzen.

Hände weg von sensiblen Daten: Die Verwendung besonders schützenswerter Daten (Gesundheit, biometrische Merkmale wie Gesichtszüge, Stimme oder Herzfrequenz) für Marketingzwecke ist generell zu verbieten.

Immaterieller Schadenersatz bei Verstößen: Manipulation führt nicht nur zu finanziellem Schaden, sondern auch zu immateriellen Verlusten (Autonomie, Privatsphäre und psychische Beeinträchtigung). Betroffene sollten dafür Kompensationszahlungen fordern können.

Verbot von Emotionserkennung und psychografischen Profilen: Die AK fordert ein absolutes Verbot der automatisierten Erkennung von Gemütszuständen und den Einsatz dieser Daten für kommerzielle Zwecke. Der EU-Entwurf zu einem KI-Gesetz enthält bloße Hinweispflichten auf Emotionserkennung. Auch der österreichische Gesetzgeber kann aktiv werden: Eine Öffnungsklausel in der Datenschutzgrundverordnung gestattet es den Mitgliedstaaten in Bezug auf die Verarbeitung biometrischer Daten Beschränkungen einzuführen.

Kündigung so einfach wie bestellen: Die Verbraucherrechte-Richtlinie muss überarbeitet werden. Anbieter müssen verpflichtet sein, über Kündigungsbutton die Vertragsbeendigung genauso einfach zu gestalten wie die Bestellung.

So entkommen Sie den Psychotricks der Anbieter

1 Hilfreiche Tools nutzen: Genervt von den ewigen Cookie-Bannern? Plugins und AddOns können Ihnen das Leben erleichtern. Probieren Sie es mit Cookie Block (<https://github.com/dibollinger/CookieBlock#download-links>) oder Privacy Badger (<https://privacybadger.org>) – diese Browser Erweiterungen deaktivieren Cookies automatisch und ersparen dir das dauernde Wegklicken!

2 Nicht stressen lassen: „35 Personen sehen sich dieses Produkt an, du hast noch 5 Sekunden!“ Countdowns, Timer und „So viele Personen haben dieses Produkt in ihrem Warenkorb“ – in den meisten Fällen sind diese Meldungen frei erfunden. Überlegen Sie gut, ob und was Sie online einkaufen wollen. Gut für Geldbörsel und die Umwelt!

3 Nicht erpressen lassen: „Erzwungene Kontinuität“ heißt das, wenn Sie dazu gezwungen werden, ein Abo abzuschließen, ein Kundenkonto zu registrieren oder sich für einen Newsletter anzumelden. Wenn Sie Probleme mit erzwungenen Anmeldungen haben, wenden Sie sich an die AK Konsument:innenberatung oder die Internet Ombudsstelle (www.ombudsstelle.at).

4 Nicht verunsichern lassen: „Sind Sie sicher, dass Sie das Produkt kaufen wollen?“ Viele Websites arbeiten mit emotionalem Druck. Sie versuchen Sie so dazu zu bringen, sich zu registrieren, extra Produkte zu kaufen oder zusätzliche Services zu beanspruchen. Nehmen Sie kurz Abstand und so den Druck aus der Situation.